SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1 REQUISITION NUMBER	PAGE	OF
2412202TTC221	1	2

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4 ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
HSTS02-12-D-TTC221				

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b TELEPHONE NUMBER (No collect calls)	8 OFFER DUE DATE/LOCAL TIME
	Renee Grace	571227 (b)(6)	

9 ISSUED BY	CODE	10 THIS ACQUISITION IS	% FOR:
OPERATIONS SUPPORT 701 S 12th St ARLINGTON VA 20598	02	☒ UNRESTRICTED OR ☐ SET ASIDE: ☐ SMALL BUSINESS ☐ HUBZONE SMALL BUSINESS ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM ☐ ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB) ☐ 8(A)	NAICS: SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING
☐ SEE SCHEDULE	Net 30	☐	14. METHOD OF SOLICITATION ☐RFQ ☐IFB ☐RFP

15. DELIVER TO	CODE	16. ADMINISTERED BY	CODE
Office of Intelligence & Analysis Program Manager - Rex Lovelady TSA Headquarters 701 South 12th Street Arlington VA 20598		OPERATIONS SUPPORT 701 S 12th St ARLINGTON VA 20598	02

17a. CONTRACTOR/ OFFEROR	CODE	FACILITY CODE	18a. PAYMENT WILL BE MADE BY	CODE
ACCENTURE FEDERAL SERVICES LIMITED LIABILITY Attn: SCOTT POSPICHEL 11951 FREEDOM DR STE 1000 Reston VA 201905658	139727148		US Coast Guard Financial Center TSA Commercial Invoices P.O. Box 4111 Chesapeake VA 23327-4111	TSA1

TELEPHONE NO 703-9473004

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

☐ 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19 ITEM NO	20 SCHEDULE OF SUPPLIES/SERVICES	21 QUANTITY	22 UNIT	23 UNIT PRICE	24 AMOUNT
	Tax ID Number: 41-2048319 DUNS Number: 139727148 Please see Page 3 for continuation of award HSTS02-12-D-TTC221. See Section B for Loaded Labor Rates for the IDIQ. Delivery: 07/16/2012 Accounting Info: 5TV112A000D2012TVC090GE000023005400540VIM-54000000 00000000-251C-TSA DIRECT-DEF. TASK-0 Continued ... *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25 ACCOUNTING AND APPROPRIATION DATA	26. TOTAL AWARD AMOUNT (For Govt Use Only)
See schedule	$0.00

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4 FAR 52.212-3 AND 52.212-5 ARE ATTACHED ADDEND ☐ ARE ☐ ARE NOT ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4 FAR 52.212-5 IS ATTACHED ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

☒ 29. AWARD OF CONTRACT _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

30b. NAME AND TITLE OF SIGNER (Type or print)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (Type or print)	31c. DATE SIGNED
		Joseph F. Wolfinger	7-31-2012

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 5/2011)
Prescribed by GSA - FAR (48 CFR) 53.212

19 ITEM NO	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23 UNIT PRICE	24. AMOUNT
	Period of Performance: 07/31/2012 to 07/30/2017				
00001	Five year ordering period (from date of award).		JB	0.00	
	- The minimum guarantee for the contract will be (b)(4)				
	- The specific services and quantities will be identified on each Order.				
	- A combined maximum ceiling of two hundred fifty ($250,000,000.00) is established as the cumu-lative total of all orders for the entire ordering period. Obligated Amount: $0.00				
	The total amount of award: $0.00. The obligation for this award is shown in box 26.				

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED.

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY (Print)	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT (Location)	
		42c. DATE REC'D (YY/MM/DD)	42d. TOTAL CONTAINERS

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 Contract Line Items, Descriptions, and Ceilings

CLIN	SUPPLIES/SERVICES	UNIT (U.S. Dollars)	UNIT PRICE	MAX AMOUNT
0001	TTAC Infrastructure Modernization (TIM) Ordering Period: 60 months			$250,000,000.00

B.1.1 Contract Maximum Quantity and Contract Value

(a) The Government intends to award a single Indefinite Delivery Indefinite Quantity type contract.
(b) The minimum guarantee for the contract will be (b)(4)
(c) The specific services and quantities will be identified on each Order.
(d) A combined maximum ceiling of two hundred fifty million ($250,000,000.00) is established as the cumulative total of all orders for the entire ordering period.

B.2 General

The Contractor shall provide, in accordance with issued Order (also noted herein as Task Orders [TOs], all management, supervision, labor, facilities, and materials necessary to provide security support services to TSA's projects and programs on an Indefinite-Delivery-Indefinite-Quantity (IDIQ) basis. Orders may be issued on a Fixed Price (FP), Cost Reimbursement, and/or Time-and-Materials (T&M) basis. Orders will be issued in accordance with the procedures set forth herein.

B.3 Orders

Orders may be placed during the Ordering Period specified in Section B.1. However, there is no requirement for the Government to issue any Orders beyond the initial Order provided it exceeds the Minimum Guarantee and the Government is not required to place future Orders or exercise Options under Orders. This is not a multi-year contract within the meaning of FAR Part 17.1. Orders may be issued with performance periods up to twelve months and may reflect additional option periods. Orders may exceed twelve months in duration provided such issuance is consistent with applicable law, regulation and rules applicable to the funds appropriation cited in the Order. The performance period will be specified in the Order and may include option periods which extend the TO up to twelve (12) months beyond the expiration date of this contract.

B.4 Contract Pricing

B.4.1 Loaded Labor Rates Applicable to Fixed Price and Time and Materials (T&M) Orders

Orders issued on a FP or T&M basis shall be priced using the loaded labor rates that do not exceed those specified in Section B.5, Loaded Labor Rates Tables. The labor rates reflect the fully-burdened rates (including profit) for each labor category and apply to all direct labor hours.

(a) Labor. The labor rates in Section B.5 are fully-burdened hourly rates for each skill classification and apply to all direct labor hours. The fully-burdened labor rates include all direct, indirect, general and administrative costs and profit associated with providing the required skill. The fully-burdened labor rates include all labor and labor-related costs, such as, but not limited to, the following list of representative labor-related costs: salaries, wages, bonuses to include stock bonuses, incentive awards, employee stock options, stock appreciation rights, employee stock ownership plans, employee insurance, fringe benefits, contributions to pension, other post-retirement benefits, annuity, employee incentive compensation plans, incentive pay, shift differentials, overtime, vacation time, sick pay, holidays, and all other allowances that should be included in a comprehensive employee compensation plan. The Government requires the contractor to state how many hours is their equivalent to a full time employee.

(1) Government Site Rates. These rates shall be used when contractor personnel are performing at Government site. The Government will provide reasonable work space, furniture, equipment and supplies, as specified in the individual Orders.

(2) Contractor Site Rates. These rates shall be used when contractor personnel are performing at the Contractor's own facility/site. The Contractor shall furnish all office space, supplies, materials and services required to perform the work. This includes, but is not limited to, telephones, faxes, copiers, personal computers, postage (to include courier services such as Federal Express), ordinary business software (e.g., word processing, spreadsheets, graphics, etc.), normal copying and reproduction costs.

(3) Other Direct Costs. The Other Direct Costs (ODCs) are for order-related travel. The cost of general-purpose items required for the conduct of the Contractor's normal business operations will not be considered an allowable ODC in the performance of orders under this contract. Only travel authorized in writing by the COTR prior to expenditure shall be reimbursed.

B.4.1.1 Fixed Price Task Orders (TOs)

For FFP type task orders, the quantity of each item or labor category ordered as negotiated for the task will be multiplied against the rate(s) listed in this schedule, and the cumulative extended total of all items ordered will define the lump sum fixed price for the TO. Discounts from these rates may be obtained at the time of negotiation. Travel costs will be in accordance with the Federal Travel Regulations (FTR), if applicable, and may be estimated for each TO and will be funded on a NTE basis. Travel shall remain separate from the total fixed price for labor and ODCs and will be reimbursed in accordance with the Federal Travel Regulation.

B.4.1.2 T&M Task Orders (TOs)

For T&M type TOs, the quantity of hours ordered from each labor category will be specified as deliverable hours billable at the ceiling rates specified in the Section B.5 Pricing Rate Tables or as negotiated, if lower rates are proposed for TO. ODCs will be estimated for each TO. Profit/fee is unallowable on ODCs. The cumulative extended total of all labor categories ordered plus ODCs will define the TO ceiling price. The government will not reimburse the Contractor for costs incurred beyond the ceiling price, for hours not delivered, for hours delivered but in excess of the quantities ordered for a particular labor category or for ODCs exceeding authorized amounts. For hours ordered but not delivered, the Government may issue a unilateral modification to the order that reduces the price of the order and de-obligates funds from the order in proportion to the number of hours ordered but not delivered. The contractor is not permitted to adjust T&M labor hours among categories after award within the overall NTE of the order, unless approved in writing by the Contracting Officer.

B.4.1.3 Cost Reimbursement Pricing

The government reserves the right to negotiate lower rates to ensure that they comply with requirements in table 15-2 in FAR 15.408 and are in accordance with any approved Defense Contract Audit Agency/Defense Contract Management Agency rates. These rates include all applicable direct and indirect rates estimates building up to the total cost.

If the TO type is to be Cost-Plus Award Fee (CPAF), the fixed portion of fee and the award portion will be clearly differentiated. Payment from the award fee pool will be based on the standards and procedures outlined in Section I.7, *Determination of Award Fee*, Section I.8, *Performance Evaluation Plan* and I.9, *Distribution of Award Fee*. Un-awarded fees shall not be rolled over into another performance period.

B.5 Loaded Labor Rates Tables

The Loaded Labor Rates Tables provide labor category descriptions, labor rates, and travel (ODCs) for performance of the requirements as specified in individual Orders. Fully loaded hourly labor rates are included for each labor category both at the Contractor site and at Government sites. These fully-loaded hourly labor rates are the maximum rates allowable for Prime Contractors and Subcontractors. These rates will be used for Firm Fixed Price and Time & Material task orders.
The contractor's labor categories shall include labor qualifications that describe required experience, certification and education. The contractor shall certify on each submitted invoice that individuals billing against a particular labor category meet the associated qualification requirements.

B.5 LOADED LABOR RATES TABLES FOR IDIQ

Labor Category – Year 1	Hourly Rate Onsite (Govt Site)	Hourly Rate Offsite (Cont Site)
Administrative Specialist - Level I	(b)(4)	
Administrative Specialist - Level II		
Communications/Network Engineer - Level I		

Communications/Network Engineer - Level II	(b)(4)
Communications/Network Engineer - Level III	
Configuration Management Specialist - Level I	
Configuration Management Specialist - Level II	
Configuration Management Specialist - Level III	
Database Administrator - Level I	
Database Administrator - Level II	
Database Administrator - Level III	
Disaster Recovery Specialist - Level I	
Disaster Recovery Specialist - Level II	
Disaster Recovery Specialist - Level III	
EVM Specialist - Level I	
EVM Specialist - Level II	
EVM Specialist - Level III	
Functional Analyst - Level I	
Functional Analyst - Level II	
Functional Analyst - Level III	
Help Desk Manager - Level II	
Help Desk Specialist - Level I	
Help Desk Specialist - Level II	
Infrastructure Engineer - Level I	
Infrastructure Engineer - Level II	
Infrastructure Engineer - Level III	
Process and Functional Analyst - Level I	
Process and Functional Analyst - Level II	
Process and Functional Analyst - Level III	
Project Control Specialist - Level I	
Project Control Specialist - Level II	
Project Control Specialist - Level III	
Project Manager - Level I	
Project Manager - Level II	
Project Manager - Level III	
Quality Assurance Manager - Level III	
Quality Assurance Specialist - Level I	
Quality Assurance Specialist - Level II	
Release Manager - Level II	
Release Manager - Level III	
Security Specialist - Level I	
Security Specialist - Level II	
Security Specialist - Level III	
Subject Matter Advisor - Level III	
Systems Administrator - Level I	
Systems Administrator - Level II	
Systems Administrator - Level III	
Systems Engineers - Level I	
Systems Engineers - Level II	
Systems Engineers - Level III	
Technical Writer/Editor - Level I	

Technical Writer/Editor - Level II	(b)(4)
Technical Writer/Editor - Level III	
Technology Architect - Level I	
Technology Architect - Level II	
Technology Architect - Level III	
Test Engineer - Level I	
Test Engineer - Level II	
Test Manager - Level II	
Test Manager - Level III	
Training Specialist - Level I	
Training Specialist - Level II	
Training Specialist - Level III	
Web Designer - Level I	
Web Designer - Level II	
Web Designer - Level III	

Labor Category – Year 2	**Hourly Rate Onsite (Govt Site)**	**Hourly Rate Offsite (Cont Site)**
Administrative Specialist - Level I	(b)(4)	
Administrative Specialist - Level II		
Communications/Network Engineer - Level I		
Communications/Network Engineer - Level II		
Communications/Network Engineer - Level III		
Configuration Management Specialist - Level I		
Configuration Management Specialist - Level II		
Configuration Management Specialist - Level III		
Database Administrator - Level I		
Database Administrator - Level II		
Database Administrator - Level III		
Disaster Recovery Specialist - Level I		
Disaster Recovery Specialist - Level II		
Disaster Recovery Specialist - Level III		
EVM Specialist - Level I		
EVM Specialist - Level II		
EVM Specialist - Level III		
Functional Analyst - Level I		
Functional Analyst - Level II		
Functional Analyst - Level III		
Help Desk Manager - Level II		
Help Desk Specialist - Level I		
Help Desk Specialist - Level II		
Infrastructure Engineer - Level I		
Infrastructure Engineer - Level II		
Infrastructure Engineer - Level III		
Process and Functional Analyst - Level I		
Process and Functional Analyst - Level II		
Process and Functional Analyst - Level III		

Project Control Specialist - Level I	(b)(4)
Project Control Specialist - Level II	
Project Control Specialist - Level III	
Project Manager - Level I	
Project Manager - Level II	
Project Manager - Level III	
Quality Assurance Manager - Level III	
Quality Assurance Specialist - Level I	
Quality Assurance Specialist - Level II	
Release Manager - Level II	
Release Manager - Level III	
Security Specialist - Level I	
Security Specialist - Level II	
Security Specialist - Level III	
Subject Matter Advisor - Level III	
Systems Administrator - Level I	
Systems Administrator - Level II	
Systems Administrator - Level III	
Systems Engineers - Level I	
Systems Engineers - Level II	
Systems Engineers - Level III	
Technical Writer/Editor - Level I	
Technical Writer/Editor - Level II	
Technical Writer/Editor - Level III	
Technology Architect - Level I	
Technology Architect - Level II	
Technology Architect - Level III	
Test Engineer - Level I	
Test Engineer - Level II	
Test Manager - Level II	
Test Manager - Level III	
Training Specialist - Level I	
Training Specialist - Level II	
Training Specialist - Level III	
Web Designer - Level I	
Web Designer - Level II	
Web Designer - Level III	

Labor Category – Year 3	**Hourly Rate Onsite (Govt Site)**	**Hourly Rate Offsite (Cont Site)**
Administrative Specialist - Level I	(b)(4)	
Administrative Specialist - Level II		
Communications/Network Engineer - Level I		
Communications/Network Engineer - Level II		
Communications/Network Engineer - Level III		
Configuration Management Specialist - Level I		
Configuration Management Specialist - Level II		

Configuration Management Specialist - Level III	(b)(4)
Database Administrator - Level I	
Database Administrator - Level II	
Database Administrator - Level III	
Disaster Recovery Specialist - Level I	
Disaster Recovery Specialist - Level II	
Disaster Recovery Specialist - Level III	
EVM Specialist - Level I	
EVM Specialist - Level II	
EVM Specialist - Level III	
Functional Analyst - Level I	
Functional Analyst - Level II	
Functional Analyst - Level III	
Help Desk Manager - Level II	
Help Desk Specialist - Level I	
Help Desk Specialist - Level II	
Infrastructure Engineer - Level I	
Infrastructure Engineer - Level II	
Infrastructure Engineer - Level III	
Process and Functional Analyst - Level I	
Process and Functional Analyst - Level II	
Process and Functional Analyst - Level III	
Project Control Specialist - Level I	
Project Control Specialist - Level II	
Project Control Specialist - Level III	
Project Manager - Level I	
Project Manager - Level II	
Project Manager - Level III	
Quality Assurance Manager - Level III	
Quality Assurance Specialist - Level I	
Quality Assurance Specialist - Level II	
Release Manager - Level II	
Release Manager - Level III	
Security Specialist - Level I	
Security Specialist - Level II	
Security Specialist - Level III	
Subject Matter Advisor - Level III	
Systems Administrator - Level I	
Systems Administrator - Level II	
Systems Administrator - Level III	
Systems Engineers - Level I	
Systems Engineers - Level II	
Systems Engineers - Level III	
Technical Writer/Editor - Level I	
Technical Writer/Editor - Level II	
Technical Writer/Editor - Level III	
Technology Architect - Level I	
Technology Architect - Level II	

Technology Architect - Level III	(b)(4)
Test Engineer - Level I	
Test Engineer - Level II	
Test Manager - Level II	
Test Manager - Level III	
Training Specialist - Level I	
Training Specialist - Level II	
Training Specialist - Level III	
Web Designer - Level I	
Web Designer - Level II	
Web Designer - Level III	

Labor Category – Year 4	**Hourly Rate Onsite (Govt Site)**	**Hourly Rate Offsite (Cont Site)**
Administrative Specialist - Level I	(b)(4)	
Administrative Specialist - Level II		
Communications/Network Engineer - Level I		
Communications/Network Engineer - Level II		
Communications/Network Engineer - Level III		
Configuration Management Specialist - Level I		
Configuration Management Specialist - Level II		
Configuration Management Specialist - Level III		
Database Administrator - Level I		
Database Administrator - Level II		
Database Administrator - Level III		
Disaster Recovery Specialist - Level I		
Disaster Recovery Specialist - Level II		
Disaster Recovery Specialist - Level III		
EVM Specialist - Level I		
EVM Specialist - Level II		
EVM Specialist - Level III		
Functional Analyst - Level I		
Functional Analyst - Level II		
Functional Analyst - Level III		
Help Desk Manager - Level II		
Help Desk Specialist - Level I		
Help Desk Specialist - Level II		
Infrastructure Engineer - Level I		
Infrastructure Engineer - Level II		
Infrastructure Engineer - Level III		
Process and Functional Analyst - Level I		
Process and Functional Analyst - Level II		
Process and Functional Analyst - Level III		
Project Control Specialist - Level I		
Project Control Specialist - Level II		
Project Control Specialist - Level III		
Project Manager - Level I		

Project Manager - Level II	(b)(4)
Project Manager - Level III	
Quality Assurance Manager - Level III	
Quality Assurance Specialist - Level I	
Quality Assurance Specialist - Level II	
Release Manager - Level II	
Release Manager - Level III	
Security Specialist - Level I	
Security Specialist - Level II	
Security Specialist - Level III	
Subject Matter Advisor - Level III	
Systems Administrator - Level I	
Systems Administrator - Level II	
Systems Administrator - Level III	
Systems Engineers - Level I	
Systems Engineers - Level II	
Systems Engineers - Level III	
Technical Writer/Editor - Level I	
Technical Writer/Editor - Level II	
Technical Writer/Editor - Level III	
Technology Architect - Level I	
Technology Architect - Level II	
Technology Architect - Level III	
Test Engineer - Level I	
Test Engineer - Level II	
Test Manager - Level II	
Test Manager - Level III	
Training Specialist - Level I	
Training Specialist - Level II	
Training Specialist - Level III	
Web Designer - Level I	
Web Designer - Level II	
Web Designer - Level III	

Labor Category – Year 5	**Hourly Rate Onsite (Govt Site)**	**Hourly Rate Offsite (Cont Site)**
Administrative Specialist - Level I	(b)(4)	
Administrative Specialist - Level II		
Communications/Network Engineer - Level I		
Communications/Network Engineer - Level II		
Communications/Network Engineer - Level III		
Configuration Management Specialist - Level I		
Configuration Management Specialist - Level II		
Configuration Management Specialist - Level III		
Database Administrator - Level I		
Database Administrator - Level II		
Database Administrator - Level III		

Disaster Recovery Specialist - Level I	(b)(4)
Disaster Recovery Specialist - Level II	
Disaster Recovery Specialist - Level III	
EVM Specialist - Level I	
EVM Specialist - Level II	
EVM Specialist - Level III	
Functional Analyst - Level I	
Functional Analyst - Level II	
Functional Analyst - Level III	
Help Desk Manager - Level II	
Help Desk Specialist - Level I	
Help Desk Specialist - Level II	
Infrastructure Engineer - Level I	
Infrastructure Engineer - Level II	
Infrastructure Engineer - Level III	
Process and Functional Analyst - Level I	
Process and Functional Analyst - Level II	
Process and Functional Analyst - Level III	
Project Control Specialist - Level I	
Project Control Specialist - Level II	
Project Control Specialist - Level III	
Project Manager - Level I	
Project Manager - Level II	
Project Manager - Level III	
Quality Assurance Manager - Level III	
Quality Assurance Specialist - Level I	
Quality Assurance Specialist - Level II	
Release Manager - Level II	
Release Manager - Level III	
Security Specialist - Level I	
Security Specialist - Level II	
Security Specialist - Level III	
Subject Matter Advisor - Level III	
Systems Administrator - Level I	
Systems Administrator - Level II	
Systems Administrator - Level III	
Systems Engineers - Level I	
Systems Engineers - Level II	
Systems Engineers - Level III	
Technical Writer/Editor - Level I	
Technical Writer/Editor - Level II	
Technical Writer/Editor - Level III	
Technology Architect - Level I	
Technology Architect - Level II	
Technology Architect - Level III	
Test Engineer - Level I	
Test Engineer - Level II	
Test Manager - Level II	

Test Manager - Level III	(b)(4)
Training Specialist - Level I	
Training Specialist - Level II	
Training Specialist - Level III	
Web Designer - Level I	
Web Designer - Level II	
Web Designer - Level III	

(End of Section B)

Transportation Security Administration

SECTION C – DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

C.1 Introduction

C.1.1 Purpose

In accordance with Federal Acquisition Regulations, a full and open competition will be sought to establish a single award Indefinite Delivery Indefinite Quantity (IDIQ) contract to support the Transportation Threat Assessment and Credentialing (TTAC) Infrastructure Modernization (TIM) Program. A single award is in the best interest of the Government. The contract requires the Contractor to work with the TIM Program in the planning, development, and implementation of the TIM system. This is accomplished by issuing Task Orders against the IDIQ contract. The task orders, while stand-alone orders, are inter-related working towards the TIM, TSA and DHS mission.

C.1.2 Background

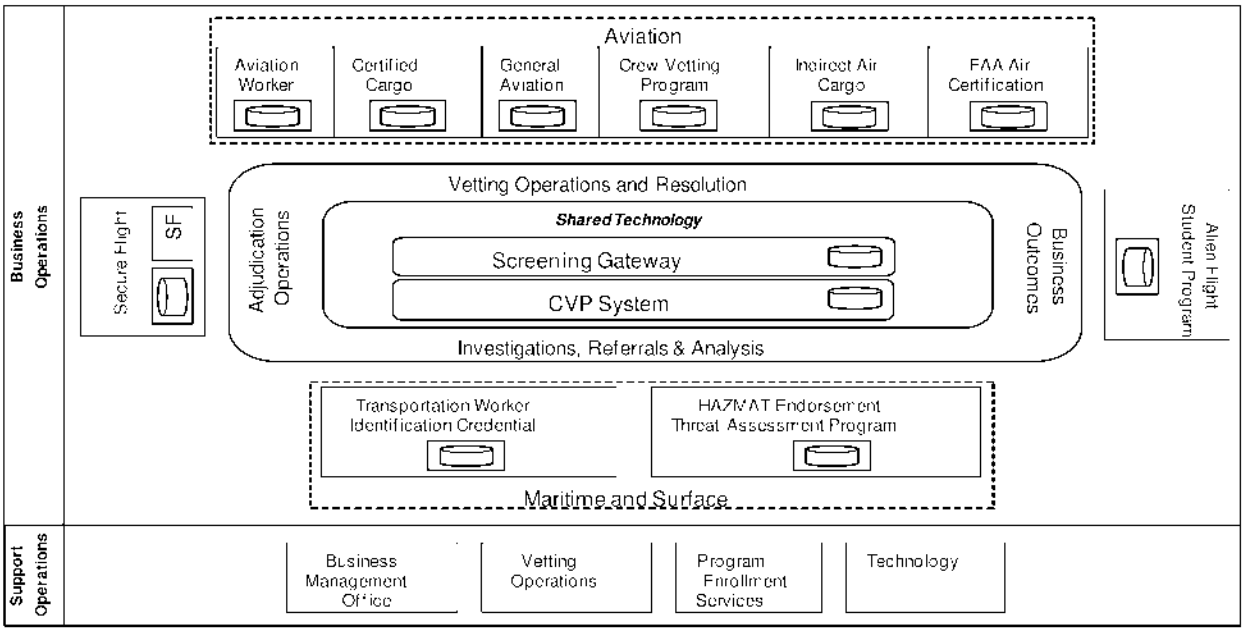
The mission of the Transportation Security Administration (TSA) is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. TSA's Office of Transportation Threat Assessment and Credentialing TTAC's mission is to reduce the probability of a successful terrorist or other criminal attack to the transportation system through application of the threat assessment methodologies that are intended to identify known or suspected terrorist or other threats working on or seeking access to the Nation's transportation system. TTAC serves as the lead for all security threat assessments and credentialing initiatives for transportation industry workers, individuals seeking access to critical infrastructure, and travelers. In support of its mission, TTAC needs to provide the following capabilities:

- Provides security threat assessments for various populations traveling into, out of, or within the United States to identify terrorist or other threats to the transportation and critical infrastructure sectors.
- Provides enrollment and credentialing services, used by an individual, to gain unescorted access to special, sterile and/or secure areas after successfully completing a security threat assessment.
- Offers screening services to support eligibility for unescorted access to special, sterile and/or secure areas where credentials may not be provided or required.
- Conducts recurrent vetting (checks daily) on over 20 million individuals against the consolidated federal watch list and other derogatory data sets.
- Engages a wide range of transportation stakeholders, requiring secure credentials, to address current and emerging threats to the transportation industry.
- Performs end-to-end program management for aviation, maritime, and surface programs with core capabilities in enrollment services, vetting operations, adjudication and credential management.

The current TTAC security threat assessment infrastructure was not built as an integrated set of capabilities to support multiple programs. The current TTAC vetting and credentialing services are limited by aging and stove piped information resource management processes and tools. The current TTAC vetting and credentialing enterprise architecture was created to support 2.5 million individuals per year. Today, the populations supported by TTAC have increased to 12.5 million individuals per year. The expected serviced populations are to grow to 20 million individuals within the next two years and a projected 40 to 50 million increases within the next five years.

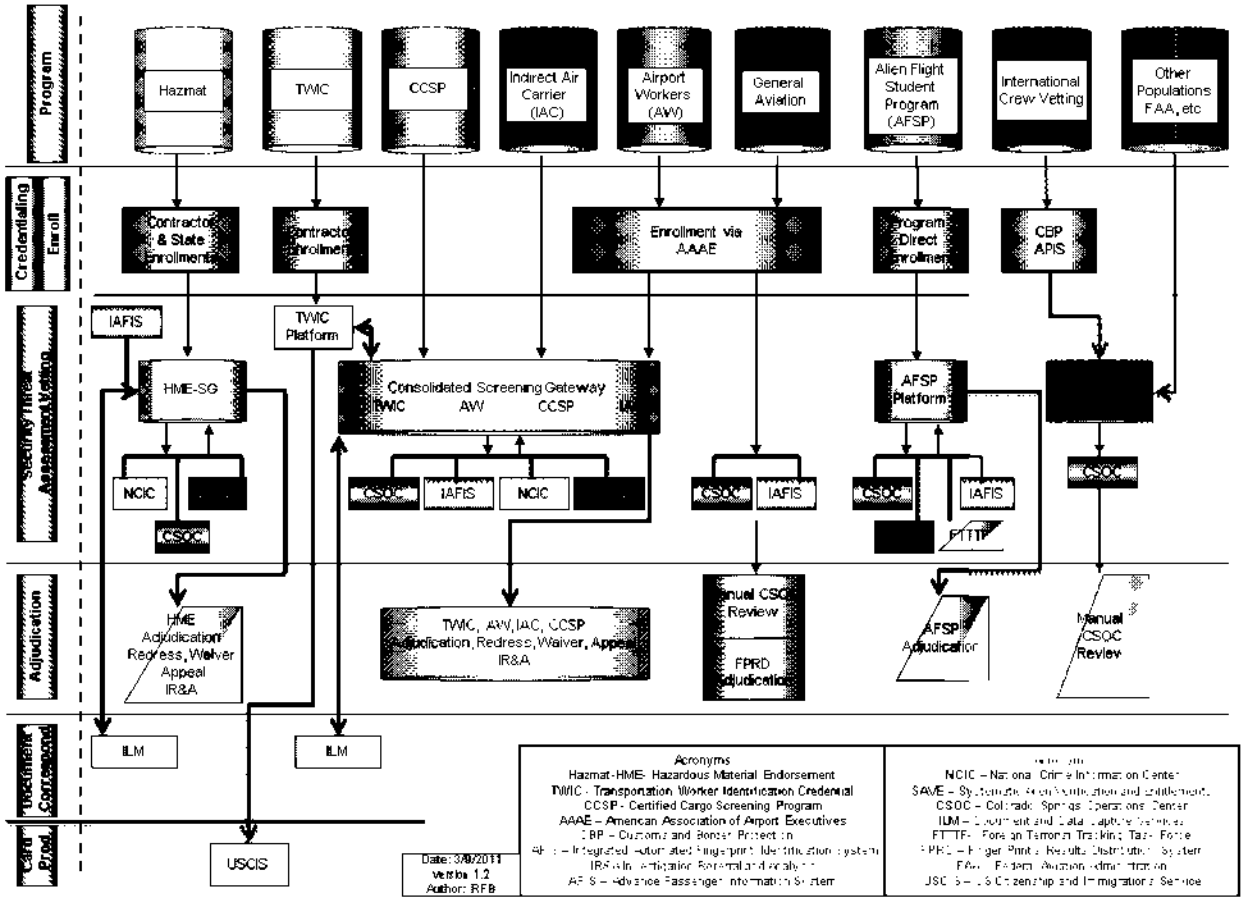
As a result, TTAC must modernize its current infrastructure to meet the TSA mission capabilities and be scalable to meet the mission needs of current and future populations.
In addition to the increase in the number of requests, it is further anticipated that after five years, existing stove-piped business processes and information systems will need to be reengineered or replaced by a new integrated business architecture that will do the following: consolidate multiple enrollment methods, implement identity management services across programs, standardize the approach for customer relationship management, move to a person-centric view, standardize the physical and virtual credentialing processes, standardize threat assessment processes, standardize STA notification and verification activities, and consolidate operations by integrating program-specific Information Technology (IT) systems and business processes into a common secure vetting, adjudication and credentialing architecture and fully integrated system. Figure 1 depicts the As-Is operational architecture.

Figure 1. As-Is Operational Architecture



The current TTAC architecture has multiple enrollment stove pipes and supporting systems as depicted in Figure 2.

Figure 2. TTAC As-Is Architecture



C.2 Scope

The scope of this acquisition is to design, build, transition, and operate the new TIM system to provide capabilities and services to meet TSA's operational mission and may support other DHS mission needs as required. The TIM system shall be a flexible, agile, and scale-able architecture, based on a DHS-compliant Service Oriented Architecture framework, to support the migration of all TSA/TTAC existing populations and new populations.

At this point, the government may have additional Service Orientated Architecture (SOA), which may include the reuse of existing DHS IT architectural platform that are undetermined at this time. The Government reserves the right to modify the contract as required.

C.2.1 External Interdependent Programs

The following lists the external interdependent network services that interface with the TIM Program:

- OneNet is the DHS Wide Area Network (encrypted) composed of Verizon/AT&T leased circuits. Customs and Border Protection (CBP) is the steward for OneNet, which itself is a transition from an older multiprotocol label switching (MPLS) network infrastructure
- Data Centers 1 and 2, located in Mississippi and Virginia, are established to consolidate information technology systems and to serve as backups for each other to maintain operations of critical departmental IT systems
- US-VISIT IDENT - Automated Biometric Identification System provides a "one step" process for searching both the FBI Criminal Master File as well as all IDENT fingerprint records
- USCIS Systematic Alien Verification for Entitlements (SAVE)
- Department of Justice (DOJ) systems that include the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprints Identification System (IAFIS) and National Crime Information Center (NCIC)
- Department of Treasury, Financial Management Services Pay.gov
- Custom and Border Protection (CBP) Advance Passenger Information System (APIS)

C.2.2 Constraints

This section identifies the major constraints by which the contractor must abide during the conduct of its efforts under this SOO. The major constraints are:

- The Contractor shall utilize all current DHS, TSA and US Government policies, directives, standards, and regulations, to include OMB Circulars that are applicable to work under this Task Order. This information includes, but is not limited to, the references listed in Appendix B
- All infrastructures will reside in the DHS Data Centers (e.g., development/test, pre-production, and production environments).

- The TIM system infrastructure will be provided by the DHS Data Centers as GFE.
- The TIM system shall comply with the DHS Data Center services. For those components proposed that are not offered by the DHS Data Centers, the government will review and, if approved, will provide these components as GFE. The government encourages offerors to propose components available at the DHS Data Centers for the TIM solution.
- Architecture will be a Service Oriented Architecture (SOA) that follows the DHS SOA Framework as modified or updated
- All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as these relate to SOO
- The Contractor shall ensure that the infrastructure provides an "active-active" Continuity of Operations (COOP) capability at FOC between the two DHS Data Centers in accordance with Service Level Agreements
- The Contractor shall ensure that all data and information is protected from unauthorized use and disclosure, both at rest and in transmission, in accordance with the security policies and privacy controls of the DHS and TSA
- Any technologies proposed shall be cost-effective and support secure sharing of data/information throughout the DHS and TSA enterprise, as well as secure data sharing with other authorized federal, state, local, and tribal agencies
- Services performed under the task order(s) are subject to and shall comply with the Americans with Disabilities Act (ADA), Section 508 standards, where applicable
- DHS governance and/or standards shall take precedence over any contradictory governance and/or standards

C.2.3 Applicable Documents

The applicable documents for this SOO are listed below:

a) Acronyms – Appendix A
b) Reference Documents - Appendix B
c) TIM Program Master Schedule – Appendix C

C.3 Program Objectives

The objective of TIM IDIQ Contract is to obtain a solution that efficiently, effectively, and economically provides and maintains a standard Information Technology infrastructure to support the TSA in meeting the TSA and DHS mission. The TSA is structuring the contract in a manner that ensures that the contractor's goals and objectives are in alignment with those of TSA and DHS. Superior performance on the contractor's part will directly and indirectly link to superior TSA and DHS mission accomplishment through the economic and efficient use of information technology.

Offerors are expected to propose solutions that replace the existing stove-piped business processes and information systems by building a new integrated business and technical architecture that makes use of a DHS-compliant Service Oriented Architecture (SOA) framework that is flexible and agile that: (1) provides for the technical and business services necessary to meet all operational requirements of TTAC in-scope programs; (2) provides for interoperability with current TSA and DHS partners; (3) follows the established standards and governance provided by TSA and DHS; (4) consolidates multiple enrollment methods, (5) implements identity management services across programs; (6) standardizes customer relationship management; (7) moves to a person-centric view; (8) standardizes the physical and non-physical credentialing processes; (9) standardizes security threat assessment processes; and (10) provides for increasing population growth, new populations (with similar credentialing business process), and ad-hoc/emergent population security threat assessments.

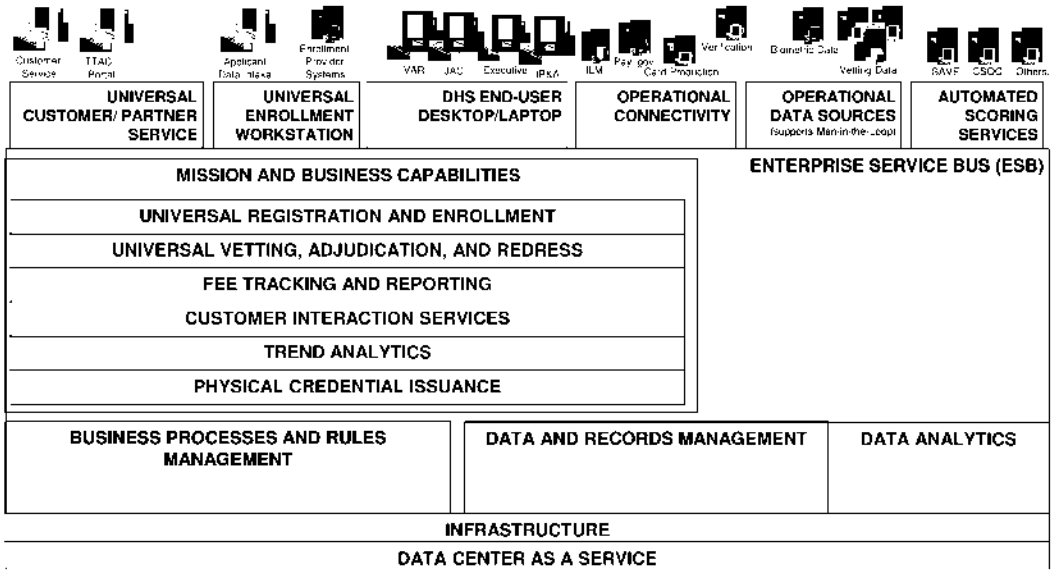
C.3.1 Objective 1: Program Management and Integration Services

Provide program management support services to efficiently manage the initial transition, the continuous evolution and the routine maintenance of the TIM system. Aspects of program management include planning, tracking of schedules, control of costs, mitigating risks, earned value management, maintaining control over configurations and quality, and meeting stakeholder expectations. The TIM Program Master Schedule is contained in Appendix C.

C.3.2 Objective 2: Systems Engineering, Architecture, and Technical Analysis

Provide comprehensive oversight of all systems engineering, architecture and technical analysis across all work areas and tasks to achieve integrated services that meet TSA mission. Figure-3 depicts the TIM Conceptual Target Architecture.

Figure 3. TIM Conceptual Target Architecture



C.3.3 Objective 3: Requirements Analysis and Definition

Gather, analyze, and document requirements to include but not limited to functional, performance, interface and data requirements for the TIM system complying with DHS SELC and NEIM.

C.3.4 Objective 4: Design, Development, Testing

Design, develop, acquire, integrate, document, secure and manage the TIM system complying with DHS SELC and NEIM.

Warehouse, inventory, transport, install, configure, integrate, test, and secure the components of the TIM system for deployment to new and existing sites. Deliver and present standard training modules to authorized users, O&M personnel, and administrators.

C.3.5 Objective 5: System Integration and Test

Provide oversight of system integration and test activities across the TIM Program to verify their suitability and effectiveness complying with program requirements, DHS SELC and NEIM.

C.3.6 Objective 6: Implementation

Prepare the system, operational environment, organizations and users for the deployment of the TIM system and evaluate operational effectiveness and suitability to determine whether the TIM system meets the mission need and operational requirements as stated in the Operational Requirements Document. Conduct operational testing and provide the security accreditation package for approval and obtain Authority to Operate.

C.3.7 Objective 7: Transition of Systems

Assume operations and maintenance of the TSA GFE legacy systems at geographically dispersed locations. Transition will also include transition of the TIM system to an Operational and Maintenance contract at the end of the IDIQ period of performance.

C.3.8 Objective 8: Operations and Maintenance

Provide operations and maintenance of the TIM system and other programs, as required, in accordance with the Service Level Agreements (SLAs) and Service Level Objectives (SLOs).
Provide local, on-site expertise with the appropriate skills, training, and experience, to include security engineering expertise, to provide operations, management, administrative, and Help Desk support for the TIM system. This includes support for the TIM system software, hardware, network infrastructure, configuration management, inventory management, network management and all tasks associated with the TIM system Continuity of Operations Plan (COOP). Maintain and update the COOP as system, business and environmental changes occur. Provide local, on-site technical expertise and Help Desk functionality to operate, maintain, and monitor all TIM

system components and external connectivity to various stakeholders and agencies. Establish the necessary Help Desk infrastructure, systems, applications and staffing to support the specified functions.

Provide local, on-site expertise with the appropriate skills, training, and experience, to include security engineering expertise, to provide technical and administrative support for Certification and Accreditation of the TIM system to achieve and maintain uninterrupted Authority to Operate (ATO) from the TSA Chief Information Officer and Chief Information Security Officer. Operate and maintain the TIM system and mission-specific infrastructures, in a manner that assures continuing ATO.
Ensure compliance with all DHS/TSA/TTAC System Security Plans. O&M of all systems will comply with TSA and TTAC security management, patch management, and configuration management plans.

C.3.9 Objective 9: Card Production Capability

The contractor shall provide the capability to produce a biometric credential to include the manufacturing and delivery of card stock, card personalization, authorization certificates, testing, analysis, and quality control in a HSPD-12 environment. The contractor shall also provide the capability to continuously adapt and comply with revised technical standards, as well as federal standards, rules, and requirements.

C.4 Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

C.4.1 Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds cus-

tom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.23 Telecommunications Products, applies to all telecommunications products including end-user interfaces such as telephones and non-end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.25 Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement.

36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

C.4.2 Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

C.4.3 Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

C.5 Travel

The cost of any Contractor travel required to comply with the IDIQ is the responsibility of the Contractor and shall be in accordance with the GSA Federal Travel Regulations. The specific travel requirements will be addressed in the individual Task Orders.

Appendix A. Acronyms

ADA	Americans with Disabilities Act
AES	Advanced Encryption Standard
AFSP	Alien Flight Student Program
ATO	Authority to Operate
AW	Aviation Workers
CBP	Customs and Border Protection
CMS	Card Management System
CONOPS	Concept of Operations
COOP	Continuity of Operations
CSG	Consolidated Screening Gateway
CVP	International Crew Vetting Program
DHS	Department of Homeland Security
DSS	Digital Signature Standard
DOJ	Department of Justice
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
GFE	Government Furnished Equipment
GSA	General Services Administration
HME	Hazardous Materials Endorsement
HSPD	Homeland Security Presidential Directive
IAC	Indirect Air Carrier
IAFIS	Integrated Automated Fingerprints Identification System
ICD	Interface Control Document
IDS	Intrusion Detection Systems
IDIQ	Indefinite Delivery Indefinite Quantity
ILSP	Integrated Logistics Support Plan
IT	Information Technology
MD	Management Directive
MNS	Mission Needs Statement
MPLS	Multiprotocol Label Switching
NCIC	National Crime Information Center
O&M	Operations and Maintenance
OMB	Office of Management and Budget
ORD	Operational Requirements Document
TIM	TTAC Infrastructure Modernization
SAVE	Systematic Alien Verification for Entitlements
SELC	Systems Engineering Life Cycle
SG	Screening Gateway
SLA	Service Level Agreement
SLO	Service Level Objectives
SOA	Service Oriented Architecture

SOO	Statement of Objectives
SOW	Statement of Work
SSI	Sensitive Security Information
STA	Security Threat Assessment
RT	Register Traveler
TSA	Transportation Security Administration
TTAC	Transportation Threat Assessment and Credentialing
TWIC	Transportation Worker Identification Credential
USCIS	US Citizenship and Immigration Services

Appendix B. Applicable Reference Documents

Executive Orders–Office of Management and Budget (OMB), Homeland Security Presidential Directive (HSPD) and Presidential Decision Directive:

- HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, 2004 http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm
- HSPD-20 National Continuity Policy, 2007 http://www.dhs.gov/xabout/laws/gc_1219245380392.shtm
- OMB Policy Memorandum M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, 2000 http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

DHS Management Directive (MD):

The DHS MDs can be accessed through the Interactive web site http://www.dhs.gov/xfoia/gc_1254501589035.shtm#4

- DHS MD 0002 Operational Integration Staff
- DHS MD 0003 Acquisition Line of Business Integration and Management
- DHS MD 0004 Administrative Service Line of Business Integration and Management
- DHS MD 0005 Financial Management Line of Business Integration and Management
- DHS MD 0006 Human Capital Line of Business Integration and Management
- DHS MD 0007.1 Information Technology Integration and Management
- DHS Acquisition Directive 102-01
- DHS MD 0480.1 Ethics/Standards of Conduct
- DHS MD 0490.1 Federal Register Notices and Rules
- DHS Directive 141-01 Record Management
- DHS MD 0560 Real Property Management Program
- DHS MD FORM 560-1 (3/05): Custody Receipt for Personal Property/ Property Pass
- DHS MD FORM 560-3 (3/05): Property Transfer Receipt
- DHS MD 0565 Personal Property Management Directive

- DHS MD 0590 Mail Management Program
- DHS MD 0731 Strategically Sourced Commodities Policy and Procedures
- DHS MD 0760.1 Purchase Card Program
- DHS MD 0780 Contracting Officer's Technical Representative (COTR) Certification, Appointment & Responsibilities
- DHS MD 0782 Acquisition Certification Requirement for Program Managers
- DHS MD 0783 Ordering Official Certification
- DHS MD 0784 Acquisition Oversight Program
- DHS MD 1120 Capitalization and Inventory of Personal Property
- DHS MD 1130.1 Electronic Funds Transfer for Disbursements, Collections and Deposits
- DHS MD 1190.1 Billings and Collections
- DHS MD 1210.1 Vendor Maintenance
- DHS MD 1330 Planning, Programming, Budgeting and Execution
- DHS MD 1510.1 Travel for Official Government Business
- DHS MD 1560.2 Payment for Official Travel Expenses by Non-Federal Sources
- DHS MD 3120.2 Employment of Non-Citizens
- DHS MD 4010.2 Section 508 Program Management Office & Electronic and Information Technology Accessibility
  - Appendix A: Software Applications and Operating Systems
  - Appendix B: Web-Based Intranet and Internet Information and Applications
  - Appendix C: Telecommunications Products
  - Appendix D: Video and Multimedia Products
  - Appendix E: Self Contained, Closed Products
  - Appendix F: Desktop and Portable Computers
  - Appendix G: Functional Performance Criteria
  - Appendix H: Information, Documentation and Support
- DHS MD 4030 Geospatial Management Office
- DHS MD 4100.1 Wireless Management Office
- DHS MD 4200.1 IT Capital Planning and Investment Control (CPIC) and Portfolio Management

- Attachment 1: Guide to Information Technology Capital Planning and Investment Control
- DHS Management Directive (MD) 4300.1 and 4300A, *Policy Guide for Sensitive Systems*
- DHS MD 4400.1 DHS Web (Internet, Intranet, and Extranet Information) and Information Systems
- DHS MD 4500.1 DHS E-Mail Usage
- DHS MD 139-01 Domain Names
- DHS MD 4600.1 Personal Use of Government Office Equipment
- DHS MD 4700.1 Personal Communications Device Distribution
- DHS MD 4800 Telecommunications Operations
  - Attachment A: Frequently Asked Questions (FAQs)
  - Attachment B: Nomination and Designation of Designated Agency Representative (DAR) for Telecommunications Services
  - Attachment C: Designated Agency Representative (DAR) for Telecommunications Services Function Requirements
- DHS MD 4900 Individual Use and Operation of DHS Information Systems/ Computers
  - Attachment A: Information Systems/Computer Access Agreement
  - Attachment B: Logon Screen
- DHS MD 8200.1 Information Quality
- DHS MD 9300.1 Continuity of Operations Programs and Continuity of Government Functions
- DHS MD 11005 Suspending Access to DHS Facilities, Sensitive Information, and IT Systems
- DHS MD 11020.1 Issuance of Access Control Media
- DHS MD 11021 Portable Electronic Devices in SCI Facilities
- DHS MD 11030.1 Physical Protection of Facilities and Real Property
- DHS MD 11041 Protection of Classified National Security Information Program Management
- DHS MD 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information
- DHS MD 11043 Sensitive Compartmented Information Program Management

- DHS MD 11044 Protection of Classified National Security Information Classification Management
- DHS MD 11045 Protection of Classified National Security Information: Accountability, Control, and Storage
- DHS MD 11046 Open Storage Area Standards for Collateral Classified Information
- DHS MD 11047 Protection of Classified National Security Information Transmission & Transportation
- DHS MD 11049 Protection of Classified National Security Information: Security Violations and Infractions
- DHS MD 11051 Department of Homeland Security SCIF Escort Procedures
- DHS MD 11052 Internal Security Program
- DHS MD 11053 Security Education, Training, and Awareness Program Directive
- DHS MD 11056.1 Sensitive Security Information (SSI)
- DHS MD 11060.1 Operations Security Program
- DHS MD 11080 Security Line of Business Integration and Management

Transportation Security Administration (TSA):

The web site http://www.tsa.dhs.gov/ contains these publications.

- TSA MD 1400.3 Information Security Policy
- TSA MD 3700.4 Handling Sensitive Personally Identifiable Information

National Institute of Standards and Technology (NIST), Special Publications:

The web site www.nist.gov contains the NIST publications

- 800-18, Guide for Developing Security Plans for Information Technology Systems, 2006
- 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, 2000
- 800-30, Risk Management Guide for Information Technology Systems, 2002
- 800-31, Intrusion Detection Systems (IDS), 2001
- 800-34, Contingency Planning Guide for Information Technology Systems, 2002
- 800-35, Guide to Information Technology Security Services, 2003
- 800-36, Guide to Selecting Information Security Products, 2003

- 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Revision 1, 2010
- 800-40, Procedures for Handling Security Patches, Version 2.0, 2005
- 800-41, Guidelines on PEPs and PEP Policy, Revision 1, 2009
- 800-45, Guidelines on Electronic Mail Security, Version 2, 2007
- 800-47, Guide for Interconnecting Information Technology Systems, 2002
- 800-50, Building an Information Technology Security Awareness and Training Program, 2003
- 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, 2002
- 800-53, Recommended Security Controls for Federal Information Systems, Revision 3, 2009
- 800-55 , Security Metrics Guide for Information Technology Systems, Revision 1, 2008
- 800-59, Guideline for Identifying an Information System as a National Security System, 2003
- 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1, 2008
- 800-61, Computer Security Incident Handling Guide, Revision 1, 2008
- 800-64, Security Considerations in the Information System Development Life Cycle, Revision 2, 2008
- 800-65, Integrating Security into the Capital Planning and Investment Control Process, 2005
- 800-68, Draft NIST Special Publication 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist, Revision 1, 2008
- 800-70, The NIST Security Configuration Checklists Program, Revision 1, 2009
- 800-94, Guide to Intrusion Detection and Prevention Systems, 2007

Federal Information Processing Standards Publications (FIPS PUBS):
The web site http://www.itl.nist.gov/fipspubs/ contains FIPS publications.

- FIPS 140-2, Security Requirements for Cryptographic Modules
- FIPS 180-3, Secure Hash Standard (SHA-1, 256, 384, and 512)
- FIPS 186-3, Digital Signature Standard (DSS)
- FIPS 197, Advanced Encryption Standard (AES)

- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, 2003
- FIPS 200, Minimum Security Requirements for Federal Employees and Contractors

Additional Citations:

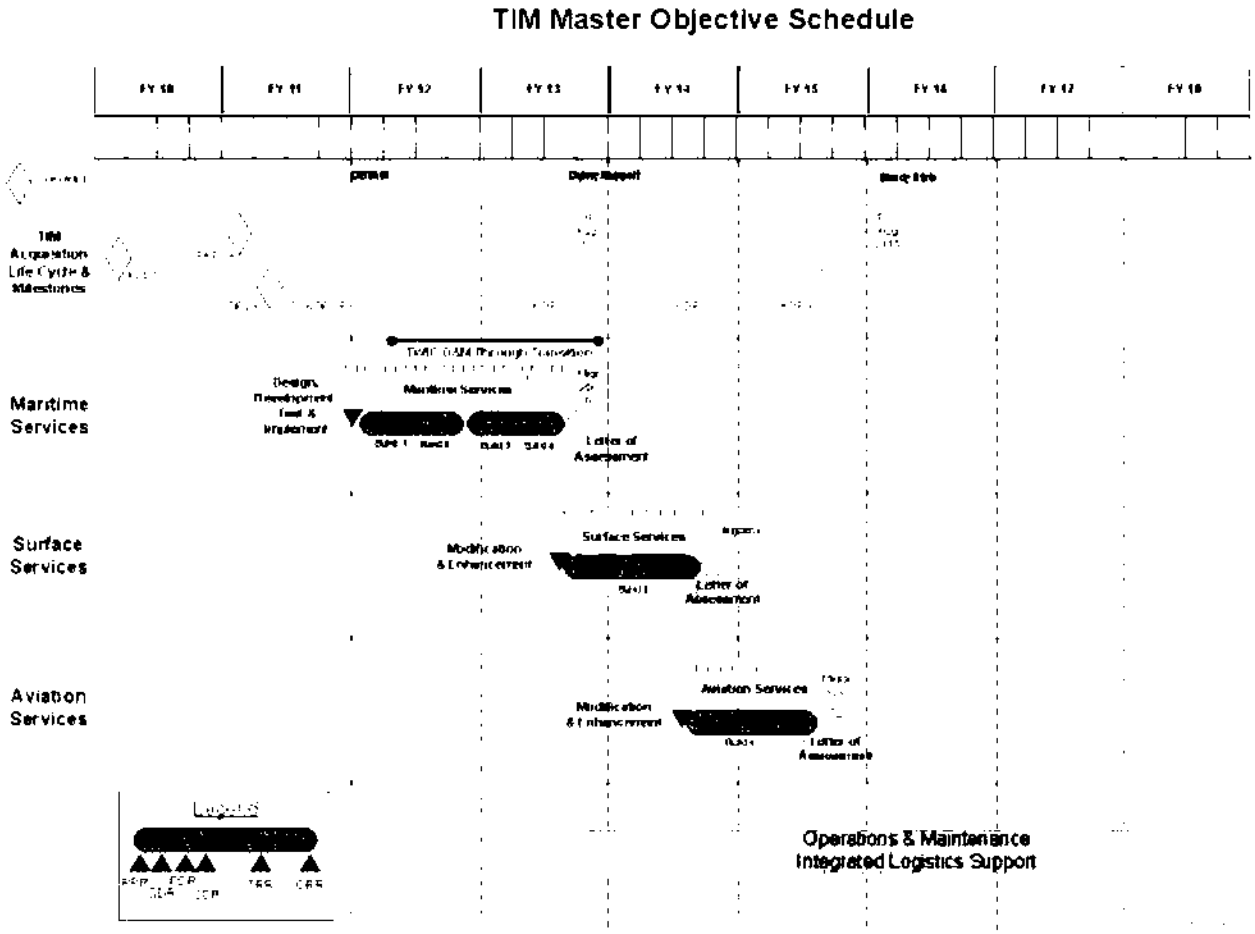
- DHS National Security Systems Policy 4300B
- DHS National Security Systems Handbook 4300B
  - Attachment A: Requirements Traceability Matrix
  - Attachment D: Certification and Accreditation Activities
  - Attachment E: FISMA Reporting
  - Attachment F: Incident Response and Reporting
- DHS Service Oriented Architecture – Technical Framework
- DHS Earned Value Management Guidance Version 1.1
- Homeland Security Enterprise Architecture (HLS EA)
- DCID 6/3, Protecting Sensitive Compartmented Information Within Information Systems http://www.dami.army.pentagon.mil/site/sso/content/Ops%20Info/DCID%206-3%20Protecting%20SCI%20Within%20Information%20Systems.pdf
- DCID 1/19 , Security Policy for Sensitive Compartmented Information and Security Policy Manual http://www.fas.org/irp/offdocs/dcid1-19.html#manual
- ISL 01L-1, Compliment to DCID 6/3, Clarification of NISPOM, chapter 8 http://www.fas.org/sgp/library/nispom/isl0101.htm
- DoD Instruction 8510.01 DoD Information Assurance Certification and Accreditation Process DIACAP) http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf
- DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) http://www.fas.org/sgp/library/nispom.htm
- Information Technology Information Library (ITIL) Process Model

Related Legislative Documents:

- Department of Homeland Security, Transportation Security Administration, U.S. Coast Guard Notice of Proposed Rulemaking (NPRM), VOL. 71, NO. 98, 22 May 06.
- The Privacy Act of 1974, U.S. Public Law 93-579, 1974
- PACS V2.2, Technical Implementation Guidance: Smart Card Enabled Physical Access Control System, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, 27 July 2004.
- Federal Information Security Management Act of 2004

- Maritime Transportation Security Act of 2002 (MTSA) Pub L. 107-295 Sec. 102 70105
- Aviation and Transportation Security Act of 2001 (ATSA) Pub. L. 107-71 Sec. 106
- USA PATRIOT Act of 2001, Pub. L 107-56 Sec. 1012

Appendix C. TIM Program Master Objective Schedule



SECTION D- PACKAGING AND MARKING

D.1 Sensitive Information Packaging and Marking

All items shall be delivered in accordance with Section D of the contract unless otherwise specified in the individual Orders.

Page Marking

Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing FOUO information with the caveat "FOR OFFICIAL USE ONLY."

Deliverables

All deliverables submitted to the Contracting Officer, the Program Manager, the COTR, the TO Program Manager, the TO Contracting Officer or the TO COTR shall be accompanied by a packing list or other suitable shipping document that shall clearly indicate the following:
(a) Contract number;
(b) Order number;
(c) Name and address of the consignor;
(d) Name and address of the consignee;
(e) Government bill of lading number covering the shipment (if any); and
(f) Description of the item/material shipped, including item number, quantity, number of containers, and package number (if any).
(g) Specific marking requirements may be addressed in individual TOs.

Specific FOUO Types

Materials containing specific types of FOUO may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions. For example:

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.*

FOUO Transmittal Outside of DHS

Materials being transmitted to recipients outside of DHS, for example, other federal agencies, state or local officials, etc. who may not be aware of what the FOUO caveat represents, shall include the following additional notice:

WARNING: *This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.*

Computer Storage Media

Computer storage media, i.e., disks, tapes, removable drives, etc., containing FOUO information will be marked "FOR OFFICIAL USE ONLY."

Classified Documents Containing FOUO

Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only FOUO information will be marked with the abbreviation (FOUO).

Individual portion markings on a document that contains no other designation are not required.

Designator or originator information and markings, downgrading instructions, and date/event markings are not required.

General Handling Procedures

Although FOUO is the DHS standard caveat for identifying sensitive unclassified information, some types of FOUO information may be more sensitive than others and thus warrant additional safeguarding measures beyond the minimum requirements established in this manual. For example, certain types of information may be considered extremely sensitive based on the repercussions that could result should the information be released or compromised. Such repercussions could be the loss of life or compromise of an informant or operation. Additional control requirements may be added as necessary to afford appropriate protection to the information. DHS employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

FOUO Coversheet Usage

When removed from an authorized storage location and persons without a need-to-know are present, or where casual observation would reveal FOUO information to unauthorized persons, a "FOR OFFICIAL USE ONLY" cover sheet will be used to prevent unauthorized or inadvertent disclosure.

Transmitting FOUO

When forwarding FOUO information, a FOUO cover sheet should be placed on top of the transmittal letter, memorandum or document.

Receiving Non-DHS and Non-TSA FOUO

When receiving FOUO equivalent information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this contract.

D.2 Requirements for Marking Sensitive Security Information (SSI)

This section contains requirements for Protective Marking and Limited Distribution Statement for Sensitive Security Information (SSI).

Protective Marking.

The protective marking consisting of the words "SENSITIVE SECURITY INFORMATION" must be applied to all documents that contain SSI. This marking should be written or stamped in plain bold type (Times New Roman) with a font size of 12 or an equivalent style and font size.

Distribution Limitation Statement

The distribution statement must be applied to all documents that contain SSI. This statement should be written or stamped in plain bold type, Times New Roman and a font size of 8 or an equivalent style and font size.

Any documents referencing Security Sensitive Information as defined in 49 CFR Part 1520 must contain the following distribution limitation statement:

"WARNING: This document contains SSI controlled under 49 CFR Part 1520. No part of this document may be released without the written permission of the Assistant Secretary of the Transportation Security, Arlington, VA. Unauthorized release may result in civil penalty (5 U.S.C 552)."

D.3 Sensitive Information Handling

The Contractor shall protect DHS sensitive information and all Government provided and contractor-owned IT systems used to store or process DHS sensitive information. The Contractor shall adhere to the following requirements for handling sensitive information:

(a) **Media Protection**. The Contractor shall ensure that all hardcopy and electronic media (including backup and removable media) that contain DHS sensitive information are appropriately marked and secured when not in use. Any sensitive

information stored on media to be surplused, transferred to another individual, or returned to the manufacturer shall be purged from the media before disposal. Disposal shall be performed using DHS approved sanitization methods. The Contractor shall establish and implement procedures to ensure sensitive information cannot be accessed or stolen. These procedures shall address the handling and protection of paper and electronic outputs from systems (computers, printers, faxes, and copiers) and the transportation and mailing of sensitive media. (See TSA 1400.3, Chapter 3, Section 19 – Information Classification, Control and Disclosure)

(b) **Access Control.** The Contractor shall control user access to DHS sensitive information based on positive user identification and authentication mechanisms. Access control measures employed shall provide protection from unauthorized alteration, loss, unavailability, or disclosure of information. The Contractor shall ensure its personnel are granted the most restrictive set of access privileges needed for performance of authorized tasks. The Contractor shall divide and separate duties and responsibilities of critical IT functions to different individuals so that no individual has all necessary authority or systems access privileges needed to disrupt or corrupt a critical process. (See TSA 1400.3, Chapter 4, Sections 2 Network Access Control, and 3 – Remote Access)

(c) **Auditing.** The Contractor shall ensure that its contractor-owned IT systems used to store or process DHS sensitive information maintain an audit trail sufficient to reconstruct security relevant events. Audit trails shall include the identity of each person and device accessing or attempting to access the system, the time and date of the access and the log-off time, activities that might modify, bypass, or negate security safeguards, and security-relevant actions associated with processing. The Contractor shall periodically review audit logs and ensure that audit trails are protected from modification, authorized access, or destruction and are retained and regularly backed up. (See TSA 1400.3, Chapter 4, Sections 10 – Security Audit Trails)

(d) **Network Security.** The Contractor shall monitor its networks for security events and employ intrusion detection systems capable of detecting inappropriate, incorrect, or malicious activity. Any interconnections between contractor-owned IT systems that process or store DHS sensitive information and IT systems not controlled by DHS shall be established through controlled interfaces and documented through formal interconnection security agreements. The Contractor shall employ boundary protection devices to enforce access control between networks, including Internet and extranet access. The Contractor shall ensure its email systems are secure, properly configured, and that network protection mechanisms implemented. The Contractor shall conduct periodic vulnerability assessments and tests on its IT systems containing DHS sensitive information to identify security vulnerabilities. (See TSA 1400.3, Chapter 4, Sections 5 – Wide Area Network (WAN) Security, and 6 – Local Area Network (LAN) Security)

(e) **Rules of Behavior.** The Contractor shall develop and enforce Rules of Behavior for contractor-owned IT systems that process or store DHS sensitive infor-

mation. (See TSA 1400.3, Chapter 3, Section 3 – Privacy and Acceptable Use Agreement)

(f) The Contractor shall adhere to the policy and guidance contained in DHS MD4300.Pub, Volume II, Part A, *IT Security Program Handbook for Sensitive Systems* in the implementation of this clause; as well as the TSA MD 1400.3 Pub Information Technology Security Manual, in above cited Sections within Chapters 2-4.

(g) All individuals that will have access to SSI under this Contract shall obtain a Non-Disclosure Agreement from the Contracting Officer.

Sources:

DHS MD4300.Pub, Volume I, Part A, *Policy Guide for Sensitive Systems*, para 3.2, *Contractors and Outsourced Operations* (2nd and 3rd policy statements)

TSA MD 1400.3 Information Technology Security Manual

D.4 Export-Sensitive Document Marking

The contractor and TSA will each mark export sensitive documents that it discloses to the other party using the following legend:

"This document contains export sensitive information. The recipient of this information is responsible for complying with all export rules of the United States Government prior to releasing or disclosing this information to nonimmigrant aliens."

D.5 Equipment Removal

All Contractor-owned equipment, accessories, and devices located on Government property shall be dismantled and removed from Government premises by the Contractor, at the Contractor's expense, within 90 calendar days after order expiration, or as mutually agreed by the Government and the Contractor. Exceptions to this requirement shall be mutually agreed upon and written notice issued by the TO Contracting Officer. Specific requirements will be addressed in individual Orders.

(End of Section D)

SECTION E- INSPECTION AND ACCEPTANCE

E.1 Inspection and Acceptance

E.1.1 Clauses Incorporated by Reference
(FAR 52.252-2) (FEB 1998)

This contract incorporates the following clauses by reference with the same force and effect as if they were given in full text. Upon request, the CO will make their full text available. Also, the full text can be accessed electronically at the following internet address: http://www.acquisition.gov/far .

FAR Clause No.	Title and Date
52.246-2	Inspection of Supplies – Fixed Price (AUG 1996)
52.246-3	Inspection of Supplies – Cost Reimbursement (MAY 2001)
52-246-4	Inspection of Services—Fixed Price (AUG 1996)
52.246-5	Inspection of Services – Cost Reimbursement (APR 1984)
52.246-6	Inspection of Services – Time and Material or Labor Hour
52.246-16	Responsibility for Supplies (APR 1984)

E.2 General

E.2.1 Inspection and acceptance of all work and services performed under each TO will be in accordance with the FAR clauses incorporated at Section E, Clauses Incorporated by Reference as applicable.

E.2.2 Final acceptance of all deliverables and or services performed as specified under each Order will be made in writing, at destination by the TO COTR or as specified in individual TOs.

E.3 Scope of Inspection

E.3.1 All deliverables will be inspected for content, completeness, and accuracy and conformance to order requirements by the TO COTR or as specified in individual Orders. Inspection may include validation of information or software through the use of automated tools and/or testing of the deliverables, as specified in the Order. The scope and nature of this testing must be negotiated prior to Task Order award and will be sufficiently comprehensive to ensure the completeness, quality and adequacy of all deliverables.

E.3.2 The Government requires a period not to exceed thirty (30) calendar days after receipt of final deliverable items for inspection and acceptance or rejection unless otherwise specified in the TO.

E.4 Basis of Acceptance

E.4.1 The basis for acceptance shall be compliance with the requirements set forth in the statement of work, the TO, the Contractor's proposal and other terms and conditions of this contract. Deliverable items rejected under any resulting Order shall be corrected in accordance with the applicable clauses.

E.4.2 Commercial and non-developmental hardware items, software items, pre-packaged solutions, and maintenance and support solutions will be accepted within thirty (30) calendar days of delivery when performance is in accordance with delivery requirements.

E.4.3 Reports, documents and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected.

E.4.4 Non-conforming products or services will be rejected. Unless otherwise agreed by the parties, deficiencies will be corrected within 30 calendar days of the rejection notice. If the deficiencies cannot be corrected within 30 days, the Contractor will immediately notify the TO Contracting Officer of the reason for the delay and provide a proposed corrective action plan within 10 working days.

E.5 Review of Deliverables

E.5.1 The Government will provide written acceptance, comments and/or change requests, if any, within fifteen (15) business days from receipt by the Government of the initial deliverable.

E.5.2 Upon receipt of the Government comments, the Contractor shall have fifteen (15) business days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.5.3 If written acceptance, comments and/or change requests are not issued by the Government within 30 calendar days of submission, the draft deliverable shall be deemed acceptable as written and the Contractor may proceed with the submission of the final deliverable product.

(End of Section E)

SECTION F- DELIVERIES OR PERFORMANCE

F.1 Clauses Incorporated by Reference
(FAR 52.252-2) (FEB 1998)

This contract incorporates the following clauses by reference with the same force and effect as if they were given in full text. Upon request, the CO will make their full text available. Also, the full text can be accessed electronically at the following internet address: http://www.acquisition.gov/far .

52.242-15 Stop-Work Order (AUG 1989)(*for other than cost reimbursement task orders*)
and ALT I (APR 1984) (*for Cost Reimbursement task orders*)
52.242.17 Government Delay of Work (APR 1984)
52.247-34 F.O.B. Destination (NOV 1991)
52.247-35 F.O.B. Destination, Within Consignee's Premises (APR 1984)

F.2 Term of the Contract

The term of this IDIQ contract is a five (5) year base period. This is not a multi-year contract as defined in FAR Part 17.1, *Multiyear Contracting*.

F.3 Task Orders Performance Period and Pricing

TOs may be issued at any time during the base and/or option periods. The performance period will be specified in the TO and may include option periods which extend the TO up to twelve (12) months beyond the expiration date of this contract. TOs, when applicable, shall be priced using the rates provided in Section B, *Supplies or Services and Price/Costs*, that will be applicable to the TO's anticipated period of performance.

F.4 – Reserved
F.5 Delivery

The services required under each individual TO shall be delivered and received at destination within the time frame specified in each order.

F.6 Place of Performance

Place of performance shall be set forth in individual TOs.

F.7 Notice to the Government of Delays

In the event the Contractor encounters difficulty in meeting performance requirements, or when it anticipates difficulty in complying with the contract delivery schedule or completion date, or as soon as the Contractor has knowledge that any actual or potential situation is delaying

or threatens to delay the timely performance of this contract, the Contractor shall immediately notify the TO CO and the TO COTR, in writing. This notification shall give pertinent details and this data shall be informational only in character; this provision shall not be construed as a waiver by the Government of any delivery schedule or date, or any rights or remedies provided by law or under this contract.

F.8 Transmittal Letter(s)

A copy of the transmittal letter forwarding deliverables to the specified destinations shall be identified by the specified Contract number.

F.9 Submission of Reports

The following reports are required to be delivered under this contract in accordance with the schedules stated and to the addresses provided for the Contracting Officer and COTR:

None specified

Order-Specific Reports

` Specific reports will be identified as required in individual Orders.

F.10 Order Process

The Government will order any supplies and services via Orders.

Orders

Only the Contracting Officer is authorized to issue Orders. The Contractor is hereby notified that future Orders may be subject to negotiations and mutual agreement of the parties.

Deliverables

All deliverables will be identified in individual Orders.

Contract Type of Orders

Orders may be *firm fixed price, cost plus, or time and materials.*

Order Contents

Each Order will contain the following:

- The scope and statement of work, meetings, travel and deliverables, as appropriate.
- Special reporting requirements
- Period of performance

- Applicable special provisions
- Firm fixed or not-to-exceed (NTE) total price
- Acceptance criteria

F.11 Delivery of Data

Data shall be delivered in digital format as specified in Order(s). Data shall be addressed to the designated Contracting Officer's Technical Representative (COTR).

(End of Section F)

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 Accounting and Appropriation Data

Accounting and appropriation data for obligations under this contract will be set forth on individual Orders.

G.2 Authority of Government Contracting Officials

The authority and roles of the Contracting Officer, Contract Specialist, and Contracting Officer's Technical Representative are as follows:

Contracting Officer: ***Renee Grace,*** (b)(6) ***571-227*** (b)(6)

The Contracting Officer has the overall and primary responsibility for the administration of this contract. Only the Contracting Officer has authority to enter into, administer, or terminate this contract on behalf of the Government. This includes modifying and deviating from the contract terms, conditions, requirement, specifications, and delivery schedules; making final decisions involving such matters as invoice payments or other consideration due to the Government for nonperformance or unsatisfactory performance, interpreting the contract, and resolving disputes; and, terminating the contract for default or convenience. The Contracting Officer also has authority to delegate certain responsibilities to an authorized Government representative.

Contract Requirement Modification

The Contracting Officer is the only person authorized to make or approve any changes in any of the requirements of this contract. Notwithstanding any clauses contained elsewhere in this contract, the said authority remains solely with the Contracting Officer. Any changes made by the contractor at the direction of any person other than the contracting officer will be considered to have been made without authority and no adjustment will be made in the order price to cover any increase in cost incurred as a result of the change.

Delegation of Contract Administration Authority

The Contracting Officer may designate, in writing, representatives to perform functions required to administer this contract, however, any implied or expressed actions taken by those representatives must be within the limits cited within the Contracting Officer's written designations. If any individual alleges to be a representative of the contracting officer and the contractor has not received a copy of the document designating that representative's authority, the contractor shall refrain from acting upon the representative's requirements and immediately contact the contracting officer to obtain a copy of the document designating that individual as a representative of the Contracting Officer.

The Contract Specialist will assist the Contracting Officer with the tasks and details associated with the pre-award and post-award phases of the contract. The Contract Specialist does not have authority to alter the contractor's obligations or to change the contract specifications, price, terms, or conditions.

Contracting Officer's Technical Representative: Alison Young, (b)(6) (b)(6)

Contracting Officer's Technical Representative (COTR): The Contracting Officer will appoint individuals to act as authorized representatives in the monitoring and administration of this contract. This individual is designated in writing as a Contracting Officer's Technical Representative (COTR), with a copy to the Contractor. An individual designated as a COTR is authorized to perform the following functions and those functions in accordance with COTR appointment letter:

(1) Coordinate the technical aspects of this contract and inspect all required services.

(2) Certify, accept and reject invoices deemed improper for payment for the services and/or supplies rendered and allowed under the terms and conditions of this contract.

(3) Designate various individuals to assist in monitoring the performance of the contract. Such persons are not official COTRs, are NOT authorized representatives of the Contracting Officer. The COTR responsibility still remains with the COTR designated by the Contracting Officer for that given area.

The COTR will represent the Contracting Officer in the administration of technical details within the scope of this contract. The COTR is also responsible for the final inspection and acceptance of all deliverables and such other responsibilities as may be specified in the order. The COTR is not otherwise authorized to make any representations or commitments of any kind on behalf of the Contracting Officer or the Government. The COTR does not have authority to alter the contractor's obligations or to change the contract specifications, price, terms or conditions. If, as a result of technical discussions, it is desirable to modify contract obligations or the statement of work, changes will be issued in writing and signed by the Contracting Officer. The Government may change the COTR assignment at any time without prior notice to the contractor. The contractor will be notified of the change.

G.3 Contractor's Program Manager

The contractor's designated Program Manager (PM) for this Contract is:
Rex Lovelady, (b)(6) **571-227-** (b)(6)

The Contractor shall provide a Program Manager for this contract that has the authority to make any no cost contract technical, hiring and dismissal decisions, or special arrangement regarding this contract. The Program Manager shall be responsible for the overall management and coordination of this Order and shall act as the central point of contact with the Government. The Program Manager shall have full authority to act for the Contractor in the performance of the required services. The Program Manager, or a designated representative, shall meet with the COTR to discuss problem areas as they occur.

G.4 Observance of Legal Holidays and Other Absences

The Government observes the following holidays:

- New Year's Day
- Martin Luther King Birthday
- President's Day
- Memorial Day
- Independence Day
- Labor Day
- Columbus Day
- Veteran's Day
- Thanksgiving Day
- Christmas Day
- Inauguration Day (Washington, DC metropolitan area)

In addition to the days designated as holidays, the Government observes also the following days:

- Any other day designated by Federal Statute, and
- Any other day designated by Executive Order, and
- Any other day designated by President's Proclamation, such as extreme weather conditions.

When the Government grants excused absence to its employees in a specific location, assigned Contractor personnel at that same location may also be dismissed. The Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the Contracting Officer or the Contracting Officer's Technical Representative. Observance of such holidays by Government personnel shall not be a reason for the Contractor to request an extension of the period of performance, or entitlement of compensation except as set forth within the contract.

In the event the Contractor's personnel work during the holiday or other excused absences, they may be compensated by the Contractor, however, no form of holiday or other premium compensation will be considered either as a direct or indirect cost, other than their normal compensation for the time worked. For cost reimbursable and time and material (T&M) contracts, the govern-

ment will only consider as direct and/or indirect costs those efforts actually performed during the holiday or excused absences in the event contractor personnel are not dismissed. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

If consistent with its own corporate policies, the contractor may implement telework or other offsite working arrangements for its employees to accomplish the requirements of this contract in the event of inclement weather, holiday, emergencies, other government shutdowns, and/or other situations if approved by the Contracting Officer or the Contracting Officer's Technical Representative. If approved, the Contractor is solely responsible for any cost differential in performance, all liabilities that may be due to performance at an alternate location, and all resources necessary to complete such performance. Use of government-furnished computer equipment and TSA approved remote access technologies may be employed if used in accordance with applicable TSA and DHS management directives and policies.

G.5 Travel and Per Diem

The Contractor shall be reimbursed for travel costs associated with this contract. The reimbursement for those costs shall be as follows:

Travel subsistence reimbursements will be authorized under the rates and conditions under the Federal Travel Regulations.
Per diem will be reimbursed, at actual costs, not to exceed, the per diem rates set forth in the Federal Travel Regulations prescribed by General Services Administration and when applicable, Standardized Regulations Section 925 Maximum Travel Per Diem Allowances for Foreign Areas – prescribed by the Department of State.
Travel of more than 10 hours, but less than 24 hours, when no lodging is required, per diem shall be one-half of the Meals and Incidental Expenses (M&IE) rate applicable to the locations of temporary duty assignment. If more than one temporary duty point is involved, the allowance of one-half of the M&IE rate is prescribed for the location where the majority of the time is spent performing official business. The per diem allowance shall not be allowed when the period of official travel is 10 hours or less during the same calendar day.
Airfare costs in excess of the lowest rate available, offered during normal business hours are not reimbursable.
All reimbursable Contractor travel shall be authorized through the issuance of a task order executed by the Contracting Officer.

Local Travel Costs will not be reimbursed under the following circumstances:

Travel at Government installations where Government transportation is available
Travel performed for personal convenience/errands, including commuting to and from work; and
Travel costs incurred in the replacement of personnel when such replacement is accomplished for the Contractor's or employee's convenience.

G.6 Preparation of Invoices

All invoices are to be submitted to the Coast Guard Finance Center (FinCen) as described below:

Method for submitting invoices for payment (select only one method per invoice submission)

(a) The Transportation Security Administration (TSA) partners with the United States Coast Guard Finance Center for financial services in support of TSA operations, including the payment of contractor invoices. Therefore, all contractor invoices must be submitted to, and will be paid by, the U.S. Coast Guard Finance Center (FinCen).

(b) Invoices may be submitted via facsimile, U.S. Mail, or email. Contractors shall utilize ONLY ONE method per invoice submission. The submission information for each of the methods is as follows in order of preference:

1) Facsimile number is: 757-413-7314

(c) The facsimile number listed above shall be used by contractors for ORIGINAL invoice submission only. If facsimile submission is utilized, contractors shall not submit hard copies of invoices via the U.S. mail. It is the responsibility of the contractor to verify that invoices are received, regardless of the method of submission used. Contractors may inquire regarding the receipt of invoices by contacting the U.S. Coast Guard Finance Center via the methods listed in subparagraph (e) of this clause.

2) U.S. Mail:

United States Coast Guard Finance Center
TSA Commercial Invoices
P.O. Box 4111
Chesapeake, VA 23327-4111

3) Email Invoices:

FIN-SMB-TSAInvoices@uscg.mil or www.fincen.uscg.mil

(d) Upon receipt of contractor invoices, FinCen will electronically route invoices to the appropriate TSA Contracting Officer's Technical Representative and/or Contracting Officer for review and approval. Upon approval, the TSA Contracting Officer will electronically route the invoices back to FinCen. Upon receipt of approved invoices from a TSA Contracting Officer, and the subsequent certification by an Authorized Certifying Official, FinCen will initiate payment of the invoices.

(c) Payment Status: Contractors may inquire on the payment status of an invoice by any of the following means:

(1) Via the internet: https://www.fincen.uscg.mil

FinCen Customer Service Section can be reached via telephone at 1-800-564-5504 or (757) 523-6940 (Voice Option #1). The hours of operation for the Customer Service line are 8:00 AM to 5:00 PM Eastern Time, Monday through Friday. However, the Customer Service line has a voice-mail feature that is available 24 hours per day, 7 days per week.

(2) Via the Payment Inquiry Form https://www.fincen.uscg.mil/secure/payment.htm

Contractor's Contract Administration

The Contractor's contract administration shall be performed by the individual named below at the address indicated. Notification of any change in the designated individual shall be provided to the Contract Administration Office (CAO) specified in the Contract Administration Plan (CAP) within a minimum of five (5) days prior to the effective date of the change.

_____
(Name)

_____
(Title)

_____
(Street Address 1)

_____
(Street Address 2)

_____
(City/State/Zip)

_____
(Phone/Fax/E-Mail)

Remittance Address:

If contractor's remittance address is different than the mailing address appearing in Block 15.A. on page 1, contractor shall provide the following information:

REMIT TO: _____ (Name)

_____ (Street Address 1)

_____ (Street Address 2)

_____ (City, State, Zip)

(End of Section G)

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 FACILITY CLEARANCE

Access to classified information at the Top Secret/SCI level is required to support the TTAC Infrastructure Modernization contract. The Contractor shall provide special handling for TOP SECRET/SCI collateral classified and/or sensitive but unclassified (SBU) data. As such, the Contractor must possess a current facility clearance at least at the TOP SECRET/SCI level. The prime contractor is responsible for ensuring that they and any subcontractor(s) comply with the provisions of the National Industrial Security Program Operating Manual (NISPOM) and the security requirements for each task order.

H.2 SPECIAL INFORMATION TECHNOLOGY CONTRACT SECURITY REQUIREMENTS

H.2.1 Controls

The Contractor shall comply with Department of Homeland Security (DHS) and Transportation Security Administration (TSA) technical, management and operational security controls to ensure that the Government's security requirements are met. These controls are described in DHS PD 4300A and TSA MD 1400 series security policy documents and are based on the NIST 800-53 Special Publication (SP) standards.

(a) Identification Badges. All Contractor employees shall be required to obtain and wear TSA identification badges when working in TSA facilities.

(b) Computer Access Agreement. All Contractor employees (users, managers, and operators of the TSA network) must sign TSA Form 1403, Computer Access Agreement. A copy of which shall be provided to the TSA contracting officer's technical representative for retention for the duration of the contract.

(c) Personnel Security.

(1) Privileged access users are individuals who have access to an information technology (IT) system with privileges of Administrator or above and have access to sensitive network infrastructure data. Privileged access users will be appropriately screened on entry into the privileged access position and the initial screening shall be refreshed every two years,

(2) Individuals terminating voluntarily or involuntarily from a Contractor performing under contract at TSA must have an exit briefing, conducted by a supervisory or manage-

ment-level employee of the Contractor in order to identify and explain their post-employment responsibilities to the TSA.

(3) Records of exit interviews will be signed and maintained by the Contractor as part of the individual employment record for a period of not less than two years following the termination of the individual's employment.

(4) The Contractor shall notify the Contracting Officer's Technical Representative and the Contracting Officer with proposed personnel changes. Written confirmation is required. This includes, but is not limited to, name changes, resignations, terminations, and reassignments to another contract.

(5) The Contractor shall notify the TSA, in writing of any requested change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other company engagements. The Contractor shall provide the following information to TSA: full name, social security number, effective date, and reason for change.

(6) The Contracting Officer must approve all personnel replacements. Estimated completion of the necessary background investigation for employee access to government facilities and information systems is approximately 30 days from the date the completed forms are received (and acknowledged as complete) in the Security Programs Division.

(7) Failure of any Contractor personnel to pass a background investigation, without timely substitution that meets the contracts requirements, may be grounds for termination of the contract.

(d) Non-Disclosure Agreements.

(1) All TSA contractor employees and consultants must execute a DHS Form 11000-6, Sensitive But Unclassified Information Non-Disclosure Agreement (NDA) upon initial assignment to TSA and before being provided access to TSA "sensitive and/or mission critical information." The original NDA will be provided to the TSA contracting officer's technical representative for retention for the duration of the contract.

(2) The Contractor, and those operating on its behalf, shall adhere to the requirements of the nondisclosure agreement unless otherwise authorized in writing by the Contracting Officer.

(e) Performance Requirements.

(1) The Contractor shall not be liable for any injury to Government personnel or damage to Government property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

(2) Contracting Officer's Technical Representative (COTR) and IT Security Division shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

H.3 CONTRACTOR ACCESS TO INFORMATION TECHNOLOGY RESOURCES

H.3.1 Security Briefings

Before receiving access to IT resources under this contract the individual must receive a security briefing, which the COTR will arrange, and complete any non-disclosure agreement furnished by DHS.

H.3.2 Limitation of Access

The Contractor shall have access only to those areas of TSA information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

H.3.3 Termination of Access

Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

H3.4. Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

H.4 ADDITIONAL PERFORMANCE REQUIREMENTS

The Contractor shall save and hold harmless and indemnify the Government against any and all liability, claims, and costs of whatever kind and nature of injury to or death of any person or persons and for loss of damage to any property occurring in connection with, or in any way incident to, or arising out of, the unauthorized use, disclosure, theft, or distribution of any data or assets related to the contract and due to negligence on the part of the contractor.

At the expiration of the contract, the contractor shall return all TSA information and IT resources provided to the contractor during the contract, and provide a certification that all assets containing or used to process TSA information have been sanitized in accordance with the TSA MD 1400.3, TSA IT Security Policy Handbook and Technical Standards. Signed proof of sanitization should be emailed to the COTR. Addition, the contractor shall provide a master asset inventory list that reflects all assets, government furnished equipment (GFE) or non-GFE that were used to process TSA information.

The Security Certification Package contains documentation required for C&A. The package will contain the following security documentation: 1) Security Assessment Report (SAR) 2) System Security Plan (SSP) or System Security Authorization Agreement (SSAA), 3) Contingency Plan, 4) Contingency Plan Test Results, 5) Federal Information Processing Standards (FIPS) 199 Categorization, 6) Privacy Threshold Analysis (PTA), 7) E-Authentication, 8) Security Test and Evaluation (ST&E) Plan, 9)Authorization to Operate (ATO) Letter, 10) Plan of Action and Milestones (POA&M), and 11) Annual Self-Assessments. The C&A package shall document the specific procedures, training, and accountability measures in place for systems that process personally identifiable information (PII). All security compliance documents will be reviewed and approved by the Chief Information Security Officer (CISO) and the Information Assurance and Cyber Security Division (IAD), and accepted by the Contracting Officer upon creation and after any subsequent changes, before they go into effect.

Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

H.5 IDENTIFICATION OF CONTRACTOR EMPLOYEES

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

H.6 PROGRAM PERFORMANCE

The Contractor shall comply with requests to be audited and provide responses within three business days to requests for data, information, and analysis from the TSA Information Assurance and Cyber Security Division (IAD) and management, as directed by the Contracting Officer and/or COTR.

The Contractor shall provide support during the Information Assurance and Cyber Security Division (IAD) audit activities and efforts. These audit activities may include, but are not limited to the following: requests for system access for penetration testing, vulnerability scanning, incident response and forensic review.

H.7 GOVERNMENT RIGHTS

Nothing in this clause shall limit the Government's rights in any way under any other provision of the contract, including those related to the Government's right to inspect and accept the services to be performed under this contract.

H.8 PUBLICITY RESTRICTIONS

The Contractor shall not use or allow to be used any aspect of this contract for publicity, unless authorized to do so in writing by the Contracting Officer. "Publicity" means, but is not limited to, advertising (e.g. trade magazines, newspapers, Internet, radio, television etc.), communications with the media, or marketing. It is further understood that this obligation shall not expire upon completion or termination of this contract, but will continue indefinitely.

The Contractor shall include the substance of this clause, including this paragraph in each subcontract issued under this contract.

H.9 CONTINGENCY PLANNING

If performance of the contract requires that DHS data be stored or processed on Contractor-owned information systems, the Contractor shall develop and maintain contingency plans to be implemented in the event normal operations are disrupted in accordance with the Office of Management and Budget (OMB) Circular A-130, Appendix III. All contractor personnel involved with contingency planning efforts shall be identified and trained in the procedures and logistics needed to implement these plans. The Contractor shall conduct periodic tests to evaluate the effectiveness of these contingency plans. The plans shall at a minimum address emergency response, backup operations, and post-disaster recovery. Contingency planning efforts shall adhere to the guidance contained in DHS

MD4300.Pub, Volume II, Part A, *IT Security Program Handbook for Sensitive Systems including among other things:*

- *The contractor shall ensure the availability of critical resources and facilitate the COOP in an emergency situation;*
- *The contractor will test their COOP annually;*
- *The contractor shall record, track and correct any COOP deficiency and any deficiency correction that cannot be accomplished within one month of the annual test will be elevated to the Information Assurance and Cyber Security Division (IAD).*

Sources:

- DHS MD4300.Pub, Volume I, Part A, *Policy Guide for Sensitive Systems*, para 3.2, *Contractors and Outsourced Operations* (2nd and 3rd policy statements); para 4.10.2, *Disaster Recovery & Continuity of Operations.*

H.10 TRAINING AND AWARENESS

(a) The Contractor shall ensure that all contractor personnel (including subcontractor personnel) who are involved in the management, use, or operation of any IT systems that handle DHS sensitive information, receive annual training in security awareness, accepted security practices, and system rules of behavior.

(b) The Contractor shall ensure that contractor personnel (including subcontractor personnel) with significant IT security responsibilities receive specialized annual training tailored to their specific security responsibilities.

(c) The training and awareness conducted under this clause shall promote a consistent understanding of the principles and concepts of telecommunications and IT systems security as described in DHS MD4300.Pub, Volume II, Part A, IT Security Program Handbook for Sensitive Systems.

(d) DHS training and awareness resources may be available for the Contractor's use in implementing the requirements of this clause. The COTR will inform the Contractor of any available DHS training resources.

Sources:

- DHS MD4300.Pub, Volume I, Part A, *Policy Guide for Sensitive Systems*, para 3.2, *Contractors and Outsourced Operations* (2nd and 3rd policy statements); para 4.1.4, Training and Awareness

H.11 INTERRELATIONSHIP OF ASSOCIATE CONTRACTORS

The TSA may enter into contractual agreements with other Contractors (i.e., "Associate Contractors") in order to provide information technology requirements separate from the work to be per-

formed under this order, yet having links and interfaces to this order. The Contractor may be required to coordinate with other such Contractor(s) through the cognizant Contracting Officer and/or designated representative in providing suitable, non-conflicting technical and/or management interfaces and in avoidance of duplication of effort. Information on deliverables provided under separate contracts may, at the discretion of the TSA and/or other Government agencies, be provided to such other Contractor(s) for the purpose of such work.

Where the Contractor and an associate Contractor fail to agree upon action to be taken in connection with their respective responsibilities, each Contractor shall promptly bring the matters to the attention of the cognizant Contracting Officer and furnish the Contractor's recommendations for a solution. The Contractor shall not be relieved of its obligations to make timely deliveries or be entitled to any other adjustment because of failure of the Contractor and its associate to promptly refer matters to the Contracting Officer or because of failure to implement Contracting Officer directions.

Where the Contractor and Associate Contractors are required to collaborate to deliver a service; the Government will designate, in writing and prior to the definition of the task, to both Contractors, a "lead Contractor" for the project. In these cases the Associate Contractors shall also be contractually required to coordinate and collaborate with the Contractor. TSA will facilitate the mutual execution of Non-Disclosure Agreements.

Compliance with this Special Contract Requirement is included in the contract price and shall not be a basis for equitable adjustment.

H.12 AVOIDANCE OF PERSONAL SERVICES

The Government shall not supervise contractor employees. The contractor shall determine work schedules and work methodology for its employees.

H.12.1 Prohibition on Personal Services

No personal services shall be performed under this Contract. No Contractor employee will be directly supervised by the Government. All individual employee assignments, and daily work direction, shall be given by the applicable employee supervisor. If the Contractor believes any Government action or communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor shall promptly notify the Contracting Officer of this communication or action.

H.12.2 Performance of Inherently Governmental Functions

The Contractor shall not perform any inherently governmental functions under this Contract. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have

no authority to in any way change the contract and that if the other Contractor believes this communication to be a direction to change their Contract, they should notify the Contracting Officer for that contract and not carry out the direction until a clarification has been issued by the Contracting Officer

H.13 KEY PERSONNEL

The contractor shall use the key personnel set forth in its offer, upon which award of this Contract shall be based, for performance of the effort set forth under the contract. In the event that one or more of the personnel are not available, or become unavailable, the contractor shall furnish substitute personnel of equal skills, which substitutions shall be subject to approval of the contracting officer.

Key personnel on this Contract are:

(See individual Orders)

If applicable, Key personnel will also be identified in Orders with the same substitution requirements as outlined herein.

H.14 CONTRACT PERSONNEL SCREENING

H.14.1 PERSONNEL ACCESS

All Contractor personnel requiring unescorted access to TSA facilities, information systems, or information will be subject to the security procedures set forth in this contract.

H.14.2 PERIOD OF PERFORMANCE FOR CONTRACTS REQUIRING EMPLOYEE BACKGROUND CHECKS

The period of performance begins 60 days after contract award to allow for the Enter On Duty Suitability Determination. A contract modification shall be executed to revise the period of performance if the determination process is completed earlier.

H.14.3 NOTIFICATION OF CLASSIFIED CONTRACT

(a) Clearance Level. This contract requires security clearance at the CONFIDENTIAL, SECRET, TOP SECRET or TOP SECRET/SCI level.

(b) Access to Classified Information. Contractor personnel are required to have access to classified information at the CONFIDENTIAL, SECRET, TOP SECRET or TOP SECRET/SCI level. *(select one)*

(c) Place of Performance. The location of performance where classified information will be accessed, produced, safeguarded, or stored is as identified below (fill in location).

The Contractor will access classified material at TSA facilities in (*fill in location*).

The Contractor will store and safeguard classified material at the (fill in level) in support of program office requirements. If the Contractor supports other government agencies on classified contracts, the TSA classified material shall be stored alone in a separate, GSA-approved safe. Classified information pertaining to other government agencies shall not be stored with the TSA classified information.

H.14.4 SUITABILITY DETERMINATION FOR CONTRACTOR EMPLOYEES

All contractor employees seeking to provide services to TSA under a TSA contract are subject to a suitability determination to assess whether their initial employment or continued employment on a TSA contract protects or promotes the efficiency of the agency. TSA, by and through the Office of Security, Personnel Security Division (PerSec), will allow a contractor employee to commence work on a TSA contract only if a review of the contractor employee's preliminary background check is favorable. Contractor employees with unfavorable preliminary background checks will not be allowed to work on a TSA contract.

A suitability determination involves the following three phases:

Phase 1: Enter On Duty Suitability Determination: a review of a contractor employee's consumer credit report, criminal history records, and submitted security forms to determine, to the extent possible, if the contractor employee has bad debt and/or criminal offenses and/or falsification issues that would prohibit employment as a TSA contractor. This determination will include verification of citizenship for contractor employees born outside of the United States. A favorable Enter On Duty Suitability Determination is not a final suitability determination; rather, it is a preliminary review of external data sources that allows the contractor employee to commence work prior to the required background investigation being completed.

When a contractor employee is deemed suitable to commence work on a TSA contract, TSA PerSec will notify the appropriate Contracting Officer's Technical Representative (COTR) of the favorable determination. Similar notifications will be sent when a contractor employee has not passed the preliminary background check and has been deemed unsuitable.

Phase 2: Background Investigation: Once the contractor employee commences work on a TSA contract, TSA PerSec will process all submitted security forms to determine whether the contractor has previously been the subject of a federal background investigation sufficient in scope to meet TSA minimum investigative requirements. Contractor employees who have a federal investigation sufficient in scope will immediately be processed for final suitability adjudication. Those contractor employees who do not have a previous federal background investigation

sufficient in scope will be scheduled for the appropriate level background investigation through the submission of their security forms to the Office of Personnel Management (OPM).

Phase 3: Final Suitability Adjudication: TSA PerSec will complete the final suitability determination after receipt, review, and adjudication of the completed OPM background investigation. The final suitability determination is an assessment made by TSA PerSec to determine whether there is reasonable expectation that the continued employment of the TSA contractor will or will not protect or promote the efficiency of the agency. An unfavorable final suitability determination will result in a notification to the COTR that the contractor employee has been deemed unsuitable for continued contract employment and that he/she shall be removed from the TSA contract.

H.15 PROHIBITION OF INDIVIDUALS

The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

H.16 CONTRACT PERSONNEL SECURITY CLEARANCES

Staff for use on these efforts must be capable of being granted a security clearance for access to classified information and/or IT resources appropriate for the level of classification associated with the work they are to perform. Contractor personnel will be required to submit documentation, including appropriate credentialing, for access to TSA workplaces through the Security Office in order to facilitate their unencumbered entrance to appropriate TSA facilities.

H.16.1 Minimum Security Clearances

Resources engaged in systems analysis, architecture development, programming, systems administration, and hands-on application development involving actual data must be cleared at the minimum security level of Secret, or Interim Secret. Administrative staff not *directly* involved in supporting these efforts need not possess a Secret-level clearance, but must have a favorably-determined employment suitability check.

H.16.2 Future Orders

Future task orders issued under this contract may require higher clearance levels such as Top Secret (TS) or Top Secret with Sensitive Compartmented Information designation (TS/SCI). When and if such future task orders are designed and awarded, required clearance levels will be specified, and the requisite DD Form 254, Contract Security Classification Specification, will be initiated.

H.16.3 Government Approval of Contractor Staff Personnel Clearances

The Government reserves the right to determine those efforts requiring security clearances and specific staff to be cleared; *the Government must approve proposed staff requiring clearances before such staff members are used on the contract.*

The Government expects that the Contractor will use existing, cleared resources, appropriate for the clearance level required, to accomplish the work contained herein. Furthermore, vendors shall not include in their price proposals any fees incurred prior to this effort for obtaining clearances for staff currently employed by the vendor.

H.17 PHYSICAL SECURITY

The Contractor shall ensure that access to Contractor buildings, rooms, work areas and spaces, and structures that house DHS sensitive information or IT systems through which DHS sensitive information can be accessed, is limited to authorized personnel. The Contractor shall ensure that controls are implemented to deter, detect, monitor, restrict, and regulate access to controlled areas at all times. Controls shall be sufficient to safeguard IT assets and DHS sensitive information against loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters. Physical security controls shall be implemented in accordance with the policy and guidance contained in DHS MD4300.Pub, Volume II, Part A, *IT Security Program Handbook for Sensitive Systems;*

Sources:

- DHS MD4300.Pub, Volume I, Part A, *Policy Guide for Sensitive Systems*, para 3.2, *Contractors and Outsourced Operations* (2nd and 3rd policy statements); para 4.2.1, General Physical Access
- DHS MD11050.1, Physical Protection of Facilities and Real Property

H.18 HANDLING SENSITIVE INFORMATION (SSI) AND IT RESOURCES

H.18.1 Definitions

Sensitive Information means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) *Protected Critical Infrastructure Information (PCII)* as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the De-

partment of Homeland Security (including the PCII Program Manager or his/her designee). The IT Security office currently has a representative engineer who attends CIP meetings;

(2) *Sensitive Security Information (SSI),* as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee). The IT Security Office currently has an SSI Officer actively engaged in SSI related issues/concerns;

(3) *"For Official Use Only (FOUO)"* is unclassified information of a sensitive nature, and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, individual privacy under 5 U.S.C. section 552a or other programs or operations essential to the national or homeland security interest; and if provided by the Government to the contractor, is marked in such a way as to place a reasonable person on notice of its sensitive nature.

(4) *"Information Technology Resources"* include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

H.18.2 Disclosure of Information –Official Use Only

Any TSA Information made available or to which access is provided, and which is marked or should be marked "Official Use Only", shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Disclosure to anyone other than an officer or employee of the contractor or subcontractor at any tier shall require prior written approval of the TSA. Requests to make such disclosure should be addressed to the TSA contracting officer.

H.18.3 Notification of Proper Use and Penalties for Misusing "Official Use Only" Information

Each officer or employee of the contractor or subcontractor at any tier to whom "Official Use Only" information may be made available or disclosed shall be notified in writing by the contractor that "Official Use Only" information disclosed to such officer or employee can be used only for the purpose and to the extent authorized herein, and that further disclosure of any such "Official Use Only" information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. Sections 641 and 3571. Section 641 of 18 U.S.C. provides, in pertinent part, that whoever knowingly converts to his use or the use of another, or without authority sells, conveys, or disposes of any record of the United States or whoever receives the same with the intent to convert it to his use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine or imprisoned up to 10 years or both.

H.18.4 Disclosure of Technology to Non-Immigrant Alien

Disclosure of source code, technology, or documentation to a nonimmigrant alien, a type of foreign national not authorized access may be considered to be an export and export control violation by TSA. The contractor shall at all time comply with Traffic in Arms Regulation (ITAR), 22 C.F.R. parts 120 through 130, and the Export Administration Regulations (EAR), 15 C.F.R. parts 730 through 799, in the performance of this contract. In complying with these export provisions, the contractor shall determine the applicability of license exemptions; exceptions and obtain appropriate licenses or other approvals for exports of source code, technology, and documentation. The contractor shall make the same determinations where its use of non-immigrant aliens would allow them access to export sensitive information. Acquisitions involving foreign nationals or foreign entities are subject to the following provisions:

H.18.5 Use of Non-Immigrant Aliens and Non-US Companies

The contractor shall submit an explanation to the TSA contracting officer of why use of the non-immigrant alien would not violate export restrictions. The contractor shall be responsible for all regulatory record keeping requirements associated with the license and license exemption or exception. Copies of export related determinations and documentation shall be provided to TSA upon request. For export or security reasons, TSA reserves the right to exclude Offerors with a controlling degree of non U.S. ownership, and non U.S. place of business or nonimmigrant aliens from being given access to software, equipment, technology or documentation necessary to prepare an offer or to perform the contract. Offerors should be aware that obtaining an export clearance license may still be outweighed by security concerns. Any potential Offeror either having or intending to make significant use of, non US companies or personnel that are nonimmigrant aliens is encourage to consult the TSA contracting officer prior to committing resources. This clause shall flow down to subcontractors.

H.19 SECURITY OF SYSTEMS HANDLING PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY INCIDENT REPONSE (Nov 2010)

(a) Definitions.

"Breach" (may be used interchangeably with "Privacy Incident') as used in this clause means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.

"Personally Identifiable Information (PII)" as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States.

Examples of PII include: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Personally Identifiable Information (Sensitive PII)" as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. , Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(1) Driver's license number, passport number, or truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Financial information such as account numbers or Electronic Funds Transfer Information
(5) Medical Information
(6) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other Personally Identifiable information may be "sensitive" depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains Personally Identifiable Information but it is not sensitive.

(b) Systems Access. Work to be performed under this contract requires the handling of Sensitive PII. The contractor shall provide the Government access to, and information regarding systems the contractor operates on behalf of the Government under this contract, when requested by the Government, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with the Government in assuring compliance with such requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.

(c) Systems Security. In performing its duties related to management, operation, and/or access of systems containing Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in DHS Sensitive System Publication 4300A or any replacement publication and rules of conduct as described in TSA MD 3700.4

In addition, use of contractor-owned laptops or other media storage devices to process or store PII is prohibited under this contract until the contractor provides, and the contracting officer in coordination with CISO approves written certification by the contractor that the following requirements are met:

(1) Laptops employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;

(2) The contractor has developed and implemented a process to ensure that security and other applications software are kept current;

(3) Mobile computing devices utilize anti-viral software and a host-based firewall mechanism;

(4) When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS security requirements.

(5) The contractor shall maintain an accurate inventory of devices used in the performance of this contract;

(6) Contractor employee annual training and rules of conduct/behavior shall be developed, conducted/issued, and acknowledged by employees in writing. Training and rules of conduct shall address at minimum:

(i) Authorized and official use;
(ii) Prohibition against use of personally-owned equipment to process, access, or store Sensitive PII;
(iii) Prohibition against access by unauthorized users and unauthorized use by authorized users; and
(iv) Protection of Sensitive PII;

(7) All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the contracting officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.

(d) Data Security. Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure Sensitive PII when not in use and/or under the control of an authorized individual, and

when in transit to prevent unauthorized access or loss. When Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the Sensitive PII irretrievable.

The contractor shall only use Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the contracting officer. At expiration or termination of this contract, the contractor shall turn over all Sensitive PII obtained under the contract that is in its possession to the Government.

(e) Breach Response. The contractor agrees that in the event of any actual or suspected breach of Sensitive PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the contracting officer, the Contracting Officer's Technical Representative (COTR), and the TSA Director of Privacy Policy & Compliance (TSAprivacy@dhs.gov). The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties.

(f) Personally Identifiable Information Notification Requirement. The contractor has in place procedures and the capability to promptly notify any individual whose Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of the Government, based upon a risk-based analysis conducted by the Government in accordance with DHS Privacy incident Handling Guidance. Notification shall not proceed unless the Government has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to Government analysis of the breach and the terms of its instructions to the contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.

In the event that a Sensitive PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should the Government

elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing the Government for those expenses.

(g) Pass-Through of Security Requirements to Subcontractors. The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

H.20 PUBLICITY AND DISSEMINATION OF CONTRACT INFORMATION

Publicity releases or commercial advertising in connection with or referring to this contract or effort shall not be made by the Contractor unless prior written approval has been received from the Contracting Officer.

The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. Two copies of any material proposed to be published or distributed shall be submitted to the Contracting Officer.

A minimum of five full business days' notice is required for requests made in accordance with this provision.

H.21 SECURITY REQUIREMENTS

The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

H.21.1 Restrictions Upon Disclosure

The Contractor agrees to keep all information it gathers or analyzes, or information the Government in the course of this Contract furnishes, in the strictest of confidence, said information being the sole property of the Government. The Contractor also agrees that Government-provided information marked "For Official Use Only," "Confidential," or "Proprietary" must also be similarly protected and shall take all reasonable measures necessary to prohibit access to such information by any such person other than those Contractor employees needing such information to perform the work, i.e., on a need-to-know basis.

(a) The Contractor shall immediately notify the Contracting Officer in the event it determines or has reason to suspect a breach of this requirement.

(b) The Contractor shall require that all employees and consultants who are given access to such information sign a confidentiality and non-disclosure statement agreeing to safeguard the confidentiality of all such information gathered or provided to them hereunder as an integral condition of their employment.

(c) Upon the Government's request, the Contractor shall provide the Contracting Officer with plans and procedures to ensure the confidentiality and physical security of information gathered or provided hereunder.

(d) The Contractor may "gather and analyze" information that is not furnished or owned by the Government. Such information will not be subject to the restrictions in this clause.

H.21.2 Confidentiality of Data and Information

(a) In the performance of this order, the Contractor, its consultants and or subcontractors, may need access to information in the Government's possession which is encumbered with restrictions on the Government's rights to use or disclose, or that might preclude dissemination or use other than in the performance of this contract. By reason of the foregoing, the Contractor agrees that any employee, subcontractor or consultant it uses shall comply with all restrictive legends or markings on data, software, or information it uses, and further agrees not to:

(1) Knowingly disclose such data or information to others without prior written authorization from the Contracting Officer, unless that data or information has otherwise become available to the public through no action or fault of the Contractor; and

(2) Use for any purpose other than the performance of this Contract data bearing a restrictive marking or legend, unless such information or data has otherwise fallen into public domain through no action or fault of the Contractor.

(3) If work required to be performed under this Contract requires access to proprietary data of other companies, the Contractor shall use its best efforts to obtain an agreement from such other companies for such use unless such data is provided or made available to the Contractor by the Government. Two copies of any such company-to-company agreements so entered into shall be furnished promptly to the Contracting Officer. Company-to-Company agreements shall prescribe the scope of authorized use of disclosure, and other terms and conditions agreed upon between the parties.

(4) The Contractor agrees to make employees aware of the requirement to maintain confidentiality of data and information and the necessity to re-

frain from divulging either proprietary data of other companies or data obtained from the Government to unauthorized persons.

(5) The Contractor agrees to obtain from each employee connected with this contract, a written agreement that the employee will not during his/her employment by the Contractor or thereafter, disclose to others or use for his/her own benefit or the future benefit of any individual, any trade secrets, confidential information or proprietary/restricted data (to include Government "For Official Use Only") received in connection with the work under this Contract.

(6) The Contractor agrees to include the substance of this provision in all subcontracts awarded under this contract, except to the extent that:

(i) The Contractor considers the application of the prohibition of this provision to be inappropriate and unnecessary in the case of a particular subcontract.

(ii) The subcontractor provides a written statement affirming absolute unwillingness to perform absent some relief from the substance of this prohibition; or

(iii)If the Contractor encounters the situation described in 6.i and ii, the Contractor agrees to provide the Contracting officer written notice of the circumstances within ten working days of being notified by the subcontractor's unwillingness to perform. The Contractor agrees not to use any subcontractor so expressing unwillingness to perform absent any relief from the requirements of this section, unless use of an alternate subcontract source would unreasonably detract from the quality of the effort.

H.21.3 General Sensitive Information Requirements

(a) Effort to be performed by this contract may require access and protection of sensitive information and data. The Contractor shall ensure that all appropriate security and protection actions are taken, including providing cleared personnel and procedures, as required, and consistent with the TSA security requirements.

(b) The Contractor shall comply with the following TSA Management Directives and any updates, as applicable:

1. TSA Management Directive No. 2800.3, "Control of Secure Terminal Equipment (STE) Telephones.
2. TSA Management Directive No. 2800.31, "Control of Integrated Services Telephone (IST) Telephones."

3. TSA Management Directive No. 2800.5, "Foreign Travel Briefing and Contact Reporting Requirements."
4. TSA Management Directive No. 2800.8, "Information Security (INFOSEC) Program."

H.21.4 Security Policies and Directives

The Contractor is required to comply with all Government security law, policies, directives, and procedures including, but not limited to:

- Federal Information Security Management Act (FISMA)
- NIST Series 800
- Security-related DHS and TSA Management Directives
- System-specific security requirements
- Application-specific security requirements

Vendors will be responsible for identifying, evaluating, and proposing appropriately qualified staff for their respective work packages.

The TSA information security policy is an operational implementation and extension of the DHS Sensitive Systems Policy Directive 4300A. DHS 4300A provides general policy in a wide variety of areas and provides guidance to DHS Organizational Elements (OEs) for the establishment of operational policy within the OEs. DHS 4300A takes precedence in instances where there is conflict between it and TSA MD 1400.3 that is not otherwise resolved by TSA MD 1400.3, Attachment 1, Security Policy – DHS Bridge. Note that the TSA MD 1400.3 addresses additional details relating to security policies, personnel security, data encryption, and more.

The Homeland Security Acquisition Regulations (HSAR) serves as a supplement to the Federal Acquisition Regulations (FAR). The OCIO/OCISO/IT Security Office currently complies with FAR and HSAR related statements, to include "Contractor Employee Access". In addition to the above referenced HSAR document, the "TSA MD 2800.71 - Pre-employment Investigation Standard for TSA Employees and Contractors" document also references and addresses:

- SSI
- FOUO
- Sensitive Information
- Information Technology Resources,
- Background checks/analysis and administrative processes together with CO, COTR and CSO,

- Sensitive information training, computer access agreement (CAA) and security orientation briefing (are performed by the IT Security's Security Awareness, Training and Education Program) for prime or subcontractors,
- Employee Non-Disclosure Agreement (NDA) which is kept on file at IT Security, and
- Specific site/building/floor access (as arranged by the COTR and Training Coordinator).

DHS MD 11042 (date 5/11/04), Safeguarding Sensitive But Unclassified (FOUO) Information and 49 Code of Federal Regulations Part 1520.5, addresses HSAR-related information for which the OCISO is in compliant as well. The TSA FISMA dashboard scores (Green) and the judgment of the DHS Inspector General attest to our compliance with Public Law and appropriate Executive Orders.

H.21.5 Privacy or Security Safeguards

(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

(c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(d) The Contractor shall not be eligible for any award fee for any evaluation period in which there is a breach of privacy or security. Lost award fee due to a major breach of privacy or security may not be allocated to future evaluation periods.

(e) The award fee authority fee authority shall determine whether a security or privacy breach is categorized as a major security or privacy breach.

To ensure that any potential final award fee evaluation at contract completion reflects any breach of privacy or security, in an interim period, the overall award fee pool shall be reduced by the amount of the fee available for the period in which the major breach occurred if a zero fee determination was made because of a major breach of privacy or security.

H.21.6 Disposition of Government Property

Thirty (30) calendar days prior to the end of the TO period of performance, or upon

termination of the contract, the Contractor shall furnish to the TO COTR a complete inventory of all Government Property in its possession under the TO that has not been tested to destruction, completely expended in performance, or incorporated and made a part of a deliverable end item. The TO COTR will furnish disposition instructions on all listed property which was furnished or purchased under the TO.

H.22 MAJOR BREACH OF SAFETY OR SECURITY

H.22.1 Safety Breach

Safety is the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. Safety is essential to TSA and is a material part of this contract. A major breach of safety may constitute a breach of contract that entitles the Government to exercise any of its rights and remedies applicable to material parts of this contract, including termination for default. A major breach of safety must be related directly to the work on the contract. A major breach of safety is an act or omission of the Contractor that consists of an accident, incident, or exposure resulting in a fatality or mission failure; or in damage to equipment or property equal to or greater than $1 million; or in any "willful" or "repeat" violation cited by the Occupational Safety and Health Administration (OSHA) or by a state agency operating under an OSHA approved plan.

H.22.2 Security Breach

Security is the condition of safeguarding against espionage, sabotage, crime (including computer crime), or attack. A major breach of security may constitute a breach of contract that entitles the Government to exercise any of its rights and remedies applicable to material parts of this contract, including termination for default. A major breach of security may occur on or off Government installations, but must be related directly to the work on the contract. A major breach of security is an act or omission by the Contractor that results in compromise of classified information, illegal technology transfer, workplace violence resulting in criminal conviction, sabotage, compromise or denial of information technology services, equipment or property damage from vandalism greater than $250,000, or theft greater than $250,000.

NOTE: Breach of Security for the purposes of this definition should not be confused with breach of security in screening operations.

H.22.3 Reporting and Investigation

In the event of a major breach of safety or security, the Contractor shall report the breach to the Contracting Officer. If directed by the Contracting Officer, the Contractor shall conduct its own investigation and report the results to the Government. The Contractor shall cooperate with the Government investigation, if conducted.

H.22.4 Computer Security Incidents

Security Incident Reporting. The Contractor shall establish and maintain a computer incident response capability. The Contractor shall report computer security incidents in accordance with the guidance and procedures contained in DHS MD4300.Pub, Volume II, Part A, *IT Security Program Handbook for Sensitive Systems.*

Sources:

- DHS MD4300.Pub, Volume I, Part A, *Policy Guide for Sensitive Systems*, para 3.2, *Contractors and Outsourced Operations* (2nd and 3rd policy statements); para 4.10.1, *Security Incident & Violation Handling*

H.24 INSURANCE-WORK ON A GOVERNMENT INSTALLATION

The Contractor shall, at its own expense, provide and maintain during the entire performance of this Contract, at least the following kinds and minimum amounts of insurance:

H.25 WORKERS' COMPENSATION AND EMPLOYER'S LIABILITY

Contractors are required to comply with applicable Federal and State workers' compensation and occupational disease statutes. If occupational diseases are not compensable under those statutes, they shall be covered under the employer's liability section of the insurance policy, except when contract operations are so commingled with a contractor's commercial operations that it would not be practical to require this coverage. Employer's liability coverage of at least $100,000 shall be required, except in States with exclusive or monopolistic funds that do not permit workers' compensation to be written by private carriers.

General Liability

- ***Bodily Injury Liability***

  The Contracting Officer shall require bodily injury liability insurance coverage written on the comprehensive form of policy of at least $500,000 per occurrence.

- ***Property Damage Liability***

Property damage liability insurance shall be required only in special circumstances as determined by the agency.

H.26 ACCESSIBILITY

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access

to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.23 Telecommunications Products, applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.25 Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement.

36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associat-

ed with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

H.27 Subcontracting

(a) In accordance with FAR 52.244-2, *Subcontracts*, including Alternate I, if the Contractor does not have an approved purchasing system, the Contractor shall obtain written TO CO consent prior to subcontracting under a:

(1) Cost-reimbursement, T&M or L-H type contract (TO); or

(2) Firm-fixed-price contract (TO) that exceeds either the simplified acquisition threshold or 5 percent of the total estimated cost of the contract (TO).

(b) If the Contractor has an approved purchasing system and consent is not required

under paragraph (d) of FAR 52.244-2, *Subcontracts,* the Contractor nevertheless, shall obtain written TO CO consent prior to subcontract under a fixed-price arrangement where 50% or more of the task order work to be conducted by the subcontractor.

(c) If the Contractor has an approved purchasing system and consent is not required under paragraph (a) and (b), the Contractor nevertheless shall notify the TO CO within fifteen(15) calendar days in advance of entering into any (i) cost-plus-fixed-fee subcontract, or (ii) fixed-price subcontract that exceeds either the simplified acquisition threshold or 5 percent of the total estimated cost of the TO.

(1) The Contractor shall notify the appropriate TO CO within fifteen (15) calendar days in advance of placing any subcontract or modification for which consent is required under paragraph (a) or (b), including the information required by paragraphs (e)(1)(i) through (e)(1)(vii) of the FAR 52.244-2 clause.

(2) The TO CO is responsible for reviewing the Contractor's notification and supporting data to ensure that the proposed subcontract is appropriate for the risk involved, and consistent with current policy and sound business judgment prior to consent to subcontract.

(3) If the Contractor enters into any subcontract that requires consent under the clause at FAR 52.244-2, *Subcontracts*, without obtaining such consent, the Government is not required to reimburse the Contractor for any costs incurred under the subcontract prior to the date the Contractor obtains the required consent. Any reimbursement of subcontract costs incurred prior to the date the consent was obtained shall be at the sole discretion of the Government.

(d) The Contractor may add or remove Subcontractors without the express written consent of the Government provided the conditions of paragraph (a) and (b), above, are met.

(e) The Government's small business goals through subcontracting efforts for large businesses under this contract are as follows:

Type of Business	**Goal % of Total Planned Subcontracting Dollars**
Small Business (SB)	40%
Small Disadvantaged Businesses (SDB)	14.5%
Women-Owned Small Businesses (WOSB)	5%
Service-Disabled Veteran-Owned Small Business (SDVOSB)	3%
Veteran-Owned Small Business (including in SDVOSB)	3%
HUBZone	3%

(f) The Government reserves the right to require a subcontracting plan, as prescribed in FAR 52.219-9, *Small Business Subcontracting Plan*, at the task order level.

(g) When a TO solicitation requires submission of a subcontracting participation plan as part of a proposal evaluation factor, the Contractor shall submit detailed subcontracting information as instructed in the TO solicitation, and is responsible for compliance with the subcontracting plan that is negotiated and approved by the TO CO throughout the contract period.
(h) At the discretion of the TO CO, if the TO CO finds that the contractor failed to make a good faith effort to comply with its subcontracting plan upon completion of the TO performance, the TO CO may issue a final decision to the contractor to that effect, and require the payment of liquidated damages in an amount stated, or appropriate contractual remedies to be processed in accordance with FAR 19.705-7, *Liquidated Damages*.

H.28 Incorporation of Subcontracting Plan

The [*insert Contractor name*] subcontracting plan, dated [*insert date*], in response to the TIM solicitation, and submitted in accordance with FAR 52.219-9, *Small Business Subcontracting Plan*, is hereby approved and incorporated herein.

H.29 Notification Requirements Under T&M and Cost Reimbursement Contracts

Contractor notification requirements for FAR Clause 52.232-20(b), *Limitation of Cost*, FAR Clause 52.232-22 (c), *Limitation of Funds,* for CPFF and CPAF task orders, and FAR Clause 52.232-7(d), *Payments under Time and Materials and Labor-Hours,* for T&M TOs (clauses are in Section I by reference), shall be accomplished only by separate correspondence directed to the TO CO with copies to the TO COTR. No other form of "notification" (e.g., mention in any type of monthly progress or status report) will effect compliance. Further, notification to any individual other than the TO CO shall not constitute compliance with this requirement.

H.30 Architectural Compliance

All back-end system hardware and/or software must be located in the DHS Consolidated Data Center unless a waiver is approved by the DHS CIO. All DHS Wide Area Network circuits must be part of the OneNet architecture unless a waiver is approved by the DHS CIO.

DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the Contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.

• All IT hardware or software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.

• All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Mode and Enterprise Architecture Information Repository.

• In compliance with OMB mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

H.31 Data Stored/Processed at Contractor Site

Unless otherwise directed by TSA, any storage of data must be contained within the resources allocated by the Contractor to support TSA and may not be on systems that are shared with other Government or commercial clients.

(End of Section H)

SECTION I- CONTRACT CLAUSES

I.1 FAR 52.252-2 Clauses Incorporated By Reference (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text may be accessed electronically at these Internet addresses:

http://farsite.hill.af.mil/
http://www.arnet.gov

FAR Clause No.	Title and Date
52.203-5	Covenant Against Contingent Fees. (APR 1984)
52.203-6	Restrictions on Subcontractor Sales to the Government. (JUL 1995)
52.203-7	Anti-Kickback Procedures. (JUL 1995)
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity. (JAN 1997)
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity. (JAN 1997)
52.203-12	Limitation on Payments to Influence Certain Federal Transactions. (SEP 2005)

52.204.6	Data Universal Numbering System (DUNS) Number. (OCT 2003)
52.204-7	Central Contractor Registration. (JUL 2006)
52.204-8	Annual Representations and Certifications (Jan 2006)
52.204-9	Personal Identity Verification of Contractor Personnel. (JAN 2006)
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (JAN 2005)
52.215-8	Order of Precedence -- Uniform Contract Format (OCT 1997)
52.215-10	Price Reduction For Defective Cost Or Pricing Data (OCT 1997)
52.215-12	Subcontractor Cost Or Pricing Data (OCT 1997)
52.215-14	Integrity of Unit Prices (OCT 1997)
52.215-15	Pension Adjustments and Asset Reversions (OCT 2004)
52.215-18	Reversion Or Adjustment Of Plans For Postretirement Benefits (PRB) Other Than Pensions (JUL 2005)
52.215-21	Requirements For Cost Or Pricing Data Or Information Other Than Cost Or Pricing Data – Modifications (OCT 1997)
52.215-23	Limitations on Pass-Through Charges (OCT 2009)
52.216-4	Economic Price Adjustment – Labor and Material (JAN 1997)
52.216-7	Allowable Cost and Payment (DEC 2002)
52.216-8	Fixed Fee (MAR 1997)
52.216-10	Incentive Fee (MAR 1997) (Applicable to Cost Plus Incentive Fee TOs only)
52.216-16	Incentive Price Revision-Firm Target (OCT 1997) (Applicable to Fixed Price (Firm Target) Incentive TOs only)
52.216-17	Incentive Price Revision-Successive Target (OCT 1997) (Applicable to Fixed Price (Successive Target) Incentive TOs only)
52.216-18	Ordering (OCT 1995). *Fill in*: Date of award through last day of contract period, as renewed.
52.216-19	Order Limitations (OCT 1995)
52.216-22	Indefinite Quantity (OCT 1995) *Fill in*: contract expiration date plus 12 months.
52.217-8	Option to Extend Services (NOV 1999) *Fill in*: Within 60 calendar days – *Applicable at Task Order level only*
52.219-9	Small Business Subcontracting Plan (JUL 2010)
52.219-16	Liquidated Damages – Subcontracting Plan (JAN 1999)
52.222-2	Payment for Overtime Premiums (JUL 1990)
52.222-3	Convict Labor (JUN 2003)
52.222-21	Prohibition of Segregated Facilities (FEB 1999)
52.222-26	Equal Opportunity (MAR 2007)
52.222-35	Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (SEP 2006)
52.222-36	Affirmative Action for Workers with Disabilities (JUN 1998)
52.222-37	Employment Reports on Special Disabled Veterans, Veterans of the Vi-

	etnam Era, and Other Eligible Veterans (SEP 2006)
52.222-50	Combating Trafficking in Persons (FEB 2009)
52.222-54	Employment Eligibility Verification (JAN 2009)
52.222-40	Notification of Employee Rights under the National Labor Relations Act (JUN 2010)
52.223-5	Pollution Prevention and Right-To-Know Information (AUG 2003)
52.223-6	Drug-Free Workplace (MAY 2001)
52.223-10	Waste Reduction Program (AUG 2000)
52.223-14	Toxic Chemical Release Reporting (AUG 2003)
52.223-15	Energy Efficiency in Energy-Consuming Products (DEC 2007)
52.223-16	IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (DEC 2007)
52.224-1	Privacy Act Notification (APR 1984)
52.224-2	Privacy Act (APR 1984)
52.225-5	Trade Agreements (AUG 2009)
52.225-8	Duty-Free Entry (FEB 2000)
52.225-13	Restrictions on Certain Foreign Purchases (JUN 2008)
52.227-1	Authorization and Consent (DEC 2007)
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement (DEC 2007)
52.227-3	Patent Indemnity (APR 1984)
52.227-14	Rights in Data - General Alternate IV (DEC 2007)
52.227-17	Rights in Data-Special Works (DEC 2007)
52-227-19	Commercial Computer Software License (DEC 2007)
52.228-5	Insurance – Work on a Government Installation (JAN 1997)
52.228-7	Insurance Liability to Third Persons (MAR 1996)
52.229-3	Federal, State, and Local Taxes (APR 2003)
52.230-2	Cost Accounting Standards (OCT 2008)
52.230-3	Disclosure and Consistency of Cost Accounting Practices (OCT 2008)
52.230-6	Administration of Cost Accounting Standards (JUN 2010)
52.232-1	Payments (APR 1984)
52.232-7	Payments Under Time and Materials and Labor-Hour Contracts (FEB 2007)
52.232-8	Discounts for Prompt Payment (FEB 2002)
52.232-9	Limitation of Withholding of Payments (APR 1984)
52.232-11	Extras (APR 1984)
52.232-17	Interest (OCT 2008)
52.232-18	Availability of Funds (APR 1984)
52.232-19	Availability of Funds for the Next Fiscal Year (APR 1984)
52.232-20	Limitation of Cost (APR 1984)
52.232-22	Limitation of Funds (APR 1984)
52.232-23	Assignment of Claims (JAN 1986)
52.232-25	Prompt Payment (OCT 2008) ALT I (FEB 2002)
52.232-33	Payment by Electronic Funds Transfer – Central Contractor Registration

	(OCT2003)
52.233-1	Disputes (JUL 2002) ALT I (DEC 1991)
52.233-3	Protest After Award (AUG 1996) ALT I (JUN 1985)
52.233-4	Applicable Law for Breach of Contract Claim (OCT 2004)
52.237-2	Protection of Government Buildings, Equipment, and Vegetation (APR 1984)
52.237-3)	Continuity of Services (JAN 1991
52.239-1	Privacy or Security Safeguards (AUG 1996)
52.242-1	Notice of Intent to Disallow Costs (APR 1984)
52.242-3	Penalties for Unallowable Costs (MAY 2001)
52.242-4	Certification of Final Indirect Costs (JAN 1997)
52.242-13	Bankruptcy (JUL 1995)
52.243-1	Changes--Fixed-Price (AUG 1987) ALT II (APR 1984)
52.243-2	Changes – Cost Reimbursement (AUG 1987) ALT I and ALT II (APR 1984)
52.243-3	Changes–Time and Materials or Labor Hours (SEP 2000)
52.244-2	Subcontracts ALT I (JUN 2007)
52.244-5	Competition in Subcontracting (DEC 1996)
52.245-1	Government Property (AUG 2010)
52.245-2	Government Property Installation Operation Services (AUG 2010)
52.245-5	Government Property (Cost-Reimbursement, Time-and-Material, or Labor-Hour Contracts). (MAY 2004)
52.245-9	Use and Charges (AUG 2010)
52.246-25	Limitation of Liability Services (FEB 1997)
52.248-1	Value Engineering (FEB 2000)
52.249-2	Termination for Convenience of the Government (Fixed Price) (MAY 2004)
52.249-4	Termination for Convenience of the Government (Services)(Short-Form) (APR 1984)
52.249-6	Termination (Cost Reimbursement)(MAY 2004) and ALT IV (SEP 1996)
52.249-8	Default (Fixed-Price Supply and Service) (APR 1984)
52.249-14	Excusable Delays (APR 1984)
52.251-1	Government Supply Sources (AUG 2010)
52.253-1	Computer Generated Forms (JAN 1991)

I.2 Clauses Incorporated in Full Text

The following clauses are hereby incorporated in full text:

FEDERAL ACQUISTION REGULATIONS (FAR)

Required Security Clauses on Classified Contracts

As prescribed in 4.404(a), insert the following clause:

52.204-2 Security Clause Requirements (Aug 1996)

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."

(b) The Contractor shall comply with—

(1) The Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (DoD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

Security Requirements for Unclassified Information Technology Resources (HSAR 3052.204-70) (JUN 2006) ***(If required for a Task Order)***

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location.

This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within *["insert number of days"]* days after task order award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the Offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the task order as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the task order, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the task order, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after task order award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the task order as a compliance document. The contractor shall comply with the approved accreditation documentation.

Contractor Employee Access
(HSAR 3052.204-71) (JUN 2006) ***(If Required for a Task Order)***

(a) Sensitive Information, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland

Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as *"For Official Use Only"*, which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated *"sensitive"* or subject to other controls, safeguards or Protection in accordance with subsequently adopted homeland security information handling procedures.

(b) *"Information Technology Resources"* includes, but are not limited to, computer equipment, networking, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on a task order must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer under the task order. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on the task order unless the requirement is waived under Departmental procedures.

(d) The Task Order Contracting Officer may require the contractor to prohibit individuals from working on the task order if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to carelessness, insubordination, incompetence, or security concerns.

(e) Work under the task order may involve access to sensitive information. Therefore,

the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after task order performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

Alternate I
(JUNE 2006)

(g) Before receiving access to IT resources under the task order, the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in the task order or approved by the COTR in writing as necessary for performance of the work under the task order. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the Statement of Work, other terms and conditions in the task order or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the task order, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the task order for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the task order, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of
both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied

Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the task order. Any additions or deletions of non-U.S. citizens after task order award shall also be reported to the Task Order Contracting Officer.

ALTERNATE II
(JUNE 2006)

(m)Each individual employee working under the task order shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidence by a permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(n) Contractor's shall identify in their task order proposals, the names and citizenship of all non-U.S. citizens proposed to work under the task order. Any additions or deletions of non- U.S. citizens after task order award shall also be reported to the Task Order Contracting Officer.

Limitation of Future Contracting
(HSAR 3052.209-73) (JUN 2006)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective Offerors is invited to FAR Subpart 9.5 - Organizational Conflicts of Interest.

(b) The nature of this conflict is: *(1) When either the Prime contractor, core team member(s) and/or subcontractor (a) has access to procurement sensitive information that may provide it an unfair advantage in competing for some or all of the proposed effort; or (b) drafts or recommends specifications or statements of work or substantially complete statements of work; (2) the contractor reviews the work of itself or any affiliates; or (3) offers advice or planning in areas in which the contractor or any affiliates have financial interests tied to particular solutions.*

(c) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall

be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

Notification of Ownership Changes
(FAR 52.215-19) (OCT 1997)

(a) The Contractor shall make the following notifications in writing:

(1) When the Contractor becomes aware that a change in its ownership has occurred, or is certain to occur, that could result in changes in the valuation of its capitalized assets in the accounting records, the Contractor shall notify the Administrative Contracting Officer (ACO) within 30 calendar days.

(2) The Contractor shall also notify the ACO within 30 calendar days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership.

(b) The Contractor shall-

(1) Maintain current, accurate, and complete inventory records of assets and their costs;

(2) Provide the ACO or designated representative ready access to the records upon request;

(3) Ensure that all individual and grouped assets, their capitalized values, accumulated depreciation or amortization, and remaining useful lives are identified accurately before and after each of the Contractor's ownership changes; and

(4) Retain and continue to maintain depreciation and amortization schedules based on the asset records maintained before each Contractor ownership change.

(c) The Contractor shall include the substance of this clause in all subcontracts under this contract that meet the applicability requirement of FAR 15.408(k).

52.216-10 Incentive Fee.(Mar 1997) (For Incentive Fee Task Orders Only-If Applicable. Fill-ins will be completed on each task order)

(a) *General*. The Government shall pay the Contractor for performing this contract a fee determined as provided in this contract.

(b) *Target cost and target fee*. The target cost and target fee specified in the Schedule are subject to adjustment if the contract is modified in accordance with paragraph (d) of this clause.

(1) "Target cost," as used in this contract, means the estimated cost of this contract as initially negotiated, adjusted in accordance with paragraph (d) of this clause.

(2) "Target fee," as used in this contract, means the fee initially negotiated on the assumption that this contract would be performed for a cost equal to the estimated cost initially negotiated, adjusted in accordance with paragraph (d) of this clause.

(c) *Withholding of payment*. Normally, the Government shall pay the fee to the Contractor as specified in the Schedule. However, when the Contracting Officer considers that performance or cost indicates that the Contractor will not achieve target, the Government shall pay on the basis of an appropriate lesser fee. When the Contractor demonstrates that performance or cost clearly indicates that the Contractor will earn a fee significantly above the target fee, the Government may, at the sole discretion of the Contracting Officer, pay on the basis of an appropriate higher fee. After payment of 85 percent of the applicable fee, the Contracting Officer may withhold further payment of fee until a reserve is set aside in an amount that the Contracting Officer considers necessary to protect the Government's interest. This reserve shall not exceed 15 percent of the applicable fee or $100,000, whichever is less. The Contracting Officer shall release 75 percent of all fee withholds under this contract after receipt of the certified final indirect cost rate proposal covering the year of physical completion of this contract, provided the Contractor has satisfied all other contract terms and conditions, including the submission of the final patent and royalty reports, and is not delinquent in submitting final vouchers on prior years' settlements. The Contracting Officer may release up to 90 percent of the fee withholds under this contract based on the Contractor's past performance related to the submission and settlement of final indirect cost rate proposals.

(d) *Equitable adjustments*. When the work under this contract is increased or decreased by a modification to this contract or when any equitable adjustment in the target cost is authorized under any other clause, equitable adjustments in the target cost, target fee, minimum fee, and maximum fee, as appropriate, shall be stated in a supplemental agreement to this contract.

(e) Fee payable.

(1) The fee payable under this contract shall be the target fee increased by _____ [*Contracting Officer insert Contractor's participation*] cents for every dollar that the total allowable cost

is less than the target cost or decreased by _____ [*Contracting Officer insert Contractor's participation*] cents for every dollar that the total allowable cost exceeds the target cost. In no event shall the fee be greater than _____ [*Contracting Officer insert percentage*] percent or less than _____ [*Contracting Officer insert percentage*] percent of the target cost.

(2) The fee shall be subject to adjustment, to the extent provided in paragraph (d) of this clause, and within the minimum and maximum fee limitations in paragraph (e)(1) of this clause, when the total allowable cost is increased or decreased as a consequence of—

(i) Payments made under assignments; or

(ii) Claims excepted from the release as required by paragraph (h)(2) of the Allowable Cost and Payment clause.

(3) If this contract is terminated in its entirety, the portion of the target fee payable shall not be subject to an increase or decrease as provided in this paragraph. The termination shall be accomplished in accordance with other applicable clauses of this contract.

(4) For the purpose of fee adjustment, "total allowable cost" shall not include allowable costs arising out of—

(i) Any of the causes covered by the Excusable Delays clause to the extent that they are beyond the control and without the fault or negligence of the Contractor or any subcontractor;

(ii) The taking effect, after negotiating the target cost, of a statute, court decision, written ruling, or regulation that results in the Contractor's being required to pay or bear the burden of any tax or duty or rate increase in a tax or duty;

(iii) Any direct cost attributed to the Contractor's involvement in litigation as required by the Contracting Officer pursuant to a clause of this contract, including furnishing evidence and information requested pursuant to the Notice and Assistance Regarding Patent and Copyright Infringement clause;

(iv) The purchase and maintenance of additional insurance not in the target cost and required by the Contracting Officer, or claims for reimbursement for liabilities to third persons pursuant to the Insurance Liability to Third Persons clause;

(v) Any claim, loss, or damage resulting from a risk for which the Contractor has been relieved of liability by the Government Property clause; or

(vi) Any claim, loss, or damage resulting from a risk defined in the contract as unusually hazardous or as a nuclear risk and against which the Government has expressly agreed to indemnify the Contractor.

(5) All other allowable costs are included in "total allowable cost" for fee adjustment in accordance with this paragraph (e), unless otherwise specifically provided in this contract.

(f) *Contract modification*. The total allowable cost and the adjusted fee determined as provided in this clause shall be evidenced by a modification to this contract signed by the Contractor and Contracting Officer.

(g) *Inconsistencies*. In the event of any language inconsistencies between this clause and provisioning documents or Government options under this contract, compensation for spare parts or other supplies and services ordered under such documents shall be determined in accordance with this clause.

(End of clause)

Determination of Award Fee
(HSAR 3052.216-71) (DEC 2003) (For Award Fee Task Orders Only-If Applicable. Fill-ins will be completed on each task order)

(a) The Government shall evaluate contractor performance at the end of each specified evaluation period(s) to determine the amount of award. The contractor agrees that the amount of award and the award fee methodology are unilateral decisions to be made at the sole discretion of the Government.

(b) Contractor performance shall be evaluated according to a Performance Evaluation Plan. The contractor shall be periodically informed of the quality of its performance and areas in which improvements are expected.

(c) The contractor shall be promptly advised, in writing, of the determination and reasons why the award fee was or was not earned. The contractor may submit a performance self-evaluation for each evaluation period. The amount of award is at the sole discretion of the Government but any self-evaluation received within (*insert number*) days after the end of the current evaluation period will be given such consideration, as may be deemed appropriate by the Government.

(d) The Government may specify that a fee not earned during a given evaluation period may be accumulated and be available for allocation to one or more subsequent periods. In that event, the distribution of award fee shall be adjusted to reflect such allocations.

Performance Evaluation Plan
(HSAR 3052.216-72) (DEC 2003) (For Award Fee Task Orders Only-If Applicable. Fill-ins will be completed on each task order)

(a) A Performance Evaluation Plan shall be unilaterally established by the Government based on the criteria stated in the contract and used for the determination of award fee. This plan shall include the criteria used to evaluate each area and the percentage of award fee (if any) available for each area. A copy of the plan shall be provided to the contractor _____ (*insert number*) calendar days prior to the start of the first evaluation period.

(b) The criteria contained within the Performance Evaluation Plan may relate to: (1)

Technical (including schedule) requirements if appropriate; (2) Management; and (3) Cost.

(c) The Performance Evaluation Plan may, consistent with the contract, be revised unilaterally by the Government at any time during the period of performance. Notification of such changes shall be provided to the contractor_____ (*insert number*) calendar days prior to the start of the evaluation period to which the change will apply.

Distribution of Award Fee
(HSAR 3052.216-73) (DEC 2003) (For Award Fee Task Orders Only-If Applicable. Fill-ins will be completed on each task order)

(a) The total amount of award fee available under this contract is assigned according to the following evaluation periods and amounts:

Evaluation Period:
Available Award Fee:
(insert appropriate information)

(b) Payment of the base fee and award fee shall be made, provided that after payment of 85 percent of the base fee and potential award fee, the Government may withhold further payment of the base fee and award fee until a reserve is set aside in an amount that the Government considers necessary to protect its interest. This reserve shall not exceed 15 percent of the total base fee and potential award fee or $100,000, whichever is less.

(c) In the event of contract termination, either in whole or in part, the amount of award fee available shall represent a pro rata distribution associated with evaluation period activities or events as determined by the Government.

(d) The Government will promptly make payment of any award fee upon the submission by the contractor to the contracting officer's authorized representative, of a public voucher or invoice in the amount of the total fee earned for the period evaluated. Payment may be made without using a contract modification.

Small Business Subcontracting Plan Reporting
(HSAR 3052.219-70) (JUN 2006)

(a) The Contractor shall enter the information for the Subcontracting Report for Individual Contracts (formally the Standard Form 294 (SF294) and the Summary Subcontractor Report (formerly the Standard Form 295 (SF295) into the electronic Subcontracting Reporting System (eSRS) at www.esrs.gov.

(b) The Contractor shall include this clause in all subcontracts that include the clause at (FAR) 48 CFR 52.219-9.

Performance-Based Payments
(FAR 52.232-32) (JAN 2008) (For Task Orders only if applicable. Fill-ins will be completed on each task order)

(a) *Amount of payments and limitations on payments.* Subject to such other limitations and conditions as are specified in this contract and this clause, the amount of payments and limitations on payments shall be specified in the contract's description of the basis for payment.

(b) *Contractor request for performance-based payment.* The Contractor may submit requests for payment of performance-based payments not more frequently than monthly, in a form and manner acceptable to the Contracting Officer. Unless otherwise authorized by the Contracting Officer, all performance-based payments in any period for which payment is being requested shall be included in a single request, appropriately itemized and totaled. The Contractor's request shall contain the information and certification detailed in paragraphs (l) and (m) of this clause.

(c) Approval and payment of requests.

(1) The Contractor shall not be entitled to payment of a request for performance based payment prior to successful accomplishment of the event or performance criterion for which payment is requested. The Contracting Officer shall determine whether the event or performance criterion for which payment is requested has been successfully accomplished in accordance with the terms of the contract. The Contracting Officer may, at any time, require the Contractor to substantiate the successful performance of any event or performance criterion which has been or is represented as being payable.

(2) A payment under this performance-based payment clause is a contract financing payment under the Prompt Payment clause of this contract and not subject to the interest penalty provisions of the Prompt Payment Act. The designated payment office will pay approved requests on the _____ *[Contracting Officer insert day as prescribed by agency head; if not prescribed, insert "30th"]* day after receipt of the request for performance-based payment by the designated payment office. However, the designated payment office is not required to provide payment if the Contracting Officer requires substantiation as provided in paragraph (c)(1) of this clause, or inquires into the status of an event or performance criterion, or into any of the conditions listed in paragraph (e) of this clause, or into the Contractor certification. The payment period will not begin until the Contracting Officer approves the request.

(3) The approval by the Contracting Officer of a request for performance-based payment does not constitute an acceptance by the Government and does not excuse the Contractor from performance of obligations under this contract.

(d) Liquidation of performance-based payments.

(1) Performance-based finance amounts paid prior to payment for delivery of an item shall be liquidated by deducting a percentage or a designated dollar amount from the delivery payment. If the performance-based finance payments are on a delivery item basis, the liquidation amount for each such line item shall be the percent of that delivery item price that was previously paid under performance based finance payments or the designated dollar amount. If the performance-based finance payments are on a whole contract basis, liquidation shall be by either pre-designated liquidation amounts or a liquidation percentage.

(2) If at any time the amount of payments under this contract exceeds any limitation in this contract, the Contractor shall repay to the Government the excess. Unless otherwise determined by the Contracting Officer, such excess shall be credited as a reduction in the unliquidated performance-based payment balance(s), after adjustment of invoice payments and balances for any retroactive price adjustments.

(e) *Reduction or suspension of performance-based payments*. The Contracting Officer may reduce or suspend performance-based payments, liquidate performance-based payments by deduction from any payment under the contract, or take a combination of these actions after finding upon substantial evidence any of the following conditions:

(1) The Contractor failed to comply with any material requirement of this contract (which includes paragraphs (h) and (i) of this clause).

(2) Performance of this contract is endangered by the Contractor's—

(i) Failure to make progress; or

(ii) Unsatisfactory financial condition.

(3) The Contractor is delinquent in payment of any subcontractor or supplier under this contract in the ordinary course of business.

(f) Title.

(1) Title to the property described in this paragraph (f) shall vest in the Government. Vestiture shall be immediately upon the date of the first performance-based payment under this contract, for property acquired or produced before that date. Otherwise, vestiture shall occur when the property is or should have been allocable or properly chargeable to this contract.

(2) *"Property,"* as used in this clause, includes all of the following described items acquired or produced by the Contractor that are or should be allocable or

properly chargeable to this contract under sound and generally accepted accounting principles and practices:

(i) Parts, materials, inventories, and work in process;

(ii) Special tooling and special test equipment to which the Government is to acquire title under any other clause of this contract;

(iii) Nondurable (*i.e.*, noncapital) tools, jigs, dies, fixtures, molds, patterns, taps, gauges, test equipment and other similar manufacturing aids, title to which would not be obtained as special tooling under paragraph (f)(2)(ii) of this clause; and

(iv) Drawings and technical data, to the extent the Contractor or subcontractors are required to deliver them to the Government by other clauses of this contract.

(3) Although title to property is in the Government under this clause, other applicable clauses of this contract (*e.g.*, the termination or special tooling clauses) shall determine the handling and disposition of the property.

(4) The Contractor may sell any scrap resulting from production under this contract, without requesting the Contracting Officer's approval, provided that any significant reduction in the value of the property to which the Government has title under this clause is reported in writing to the Contracting Officer.

(5) In order to acquire for its own use or dispose of property to which title is vested in the Government under this clause, the Contractor shall obtain the Contracting Officer's advance approval of the action and the terms. If approved, the basis for payment (the events or performance criteria) to which the property is related shall be deemed to be not in compliance with the terms of the contract and not payable (if the property is part of or needed for performance), and the Contractor shall refund the related performance-based payments in accordance with paragraph (d) of this clause.

(6) When the Contractor completes all of the obligations under this contract, including liquidation of all performance-based payments, title shall vest in the Contractor for all property (or the proceeds thereof) not—

(i) Delivered to, and accepted by, the Government under this contract; or

(ii) Incorporated in supplies delivered to, and accepted by, the Government under this contract and to which title is vested in the Government under this clause.

(7) The terms of this contract concerning liability for Government-furnished property shall not apply to property to which the Government acquired title solely under this clause.

(g) *Risk of loss.* Before delivery to and acceptance by the Government, the Contractor shall bear the risk of loss for property, the title to which vests in the Government under this clause, except to the extent the Government expressly assumes the risk. If any property is damaged, lost, stolen, or destroyed, the basis of payment (the events or performance criteria) to which the property is related shall be deemed to be not in compliance with the terms of the contract and not payable (if the property is part of or needed for performance), and the Contractor shall refund the related performance-based payments in accordance with paragraph (d) of this clause.

(h) *Records and controls.* The Contractor shall maintain records and controls adequate for administration of this clause. The Contractor shall have no entitlement to performance-based payments during any time the Contractor's records or controls are determined by the Contracting Officer to be inadequate for administration of this clause.

(i) *Reports and Government access.* The Contractor shall promptly furnish reports, certificates, financial statements, and other pertinent information requested by the Contracting Officer for the administration of this clause and to determine that an event or other criterion prompting a financing payment has been successfully accomplished. The Contractor shall give the Government reasonable opportunity to examine and verify the Contractor's records and to examine and verify the Contractor's performance of this contract for administration of this clause.

(j) *Special terms regarding default.* If this contract is terminated under the Default clause,

(1) the Contractor shall, on demand, repay to the Government the amount of unliquidated performance-based payments, for all property for which the Government elects not to require delivery under the Default clause of this contract. The Government shall be liable for no payment except as provided by the Default clause.

(k) *Reservation of rights.*

(1) No payment or vesting of title under this clause shall—

(i) Excuse the Contractor from performance of obligations under this contract; or

(ii) Constitute a waiver of any of the rights or remedies of the parties under the contract.

(2) The Government's rights and remedies under this clause—

(i) Shall not be exclusive, but rather shall be in addition to any other rights and remedies provided by law or this contract; and

(ii) Shall not be affected by delayed, partial, or omitted exercise of any right, remedy, power, or privilege, nor shall such exercise or any single exercise preclude or impair any further exercise under this clause or the exercise of any other right, power, or privilege of the Government.

(l) *Content of Contractor's request for performance-based payment.* The Contractor's request for performance-based payment shall contain the following:

(1) The name and address of the Contractor;

(2) The date of the request for performance-based payment;

(3) The contract number and/or other identifier of the contract or order under which the request is made;

(4) Such information and documentation as is required by the contract's description of the basis for payment; and

(5) A certification by a Contractor official authorized to bind the Contractor, as specified in paragraph (m) of this clause.

(m) *Content of Contractor's certification.* As required in paragraph (l)(5) of this clause, the Contractor shall make the following certification in each request for performance-based payment:

I certify to the best of my knowledge and belief that—

(1) This request for performance-based payment is true and correct; this request (and attachments) has been prepared from the books and records of the Contractor, in accordance with the contract and the instructions of the Contracting Officer;

(2) (Except as reported in writing on _____), all payments to subcontractors and suppliers under this contract have been paid, or will be paid, currently, when due in the ordinary course of business;

(3) There are no encumbrances (except as reported in writing on _____) against the property acquired or produced for, and allocated or properly chargeable to, the contract which would affect or impair the Government's title;

(4) There has been no materially adverse change in the financial condition of the Contractor since the submission by the Contractor to the Government of the most recent written information dated _____; and

(5) After the making of this requested performance-based payment, the amount of all payments for each deliverable item for which performance-based payments have been requested will not exceed any limitation in the contract, and the amount of all payments under the contract will not exceed any limitation in the contract.

***Note*:** Contractor shall submit proposals in accordance with the provision at 52.216-30, *Time-and-Materials/Labor-Hour Proposal Requirements - Non-Commercial Item Acquisitions without Adequate Price Competition*, in solicitations for noncommercial items contemplating use of a Time-and-Materials or Labor-Hour type of contract if the price is not expected to be based on adequate price competition (if the contractor is unsure whether there will be adequate price competition, the contractor shall contact the TO CO for the specific task.)

Time-and-Materials/Labor-Hour Proposal Requirements—Non- Commercial Item Acquisition without Adequate Price Competition
(52.216-30) (FEB 2007)

(a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

(b) The Offeror must specify separate fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit for each category of labor to be performed by—

(1) The Offeror;

(2) Each subcontractor; and

(3) Each division, subsidiary, or affiliate of the Offeror under a common control.

(c) Unless exempt under paragraph (d) of this provision, the fixed hourly rates for services transferred between divisions, subsidiaries, or affiliates of the Offeror under a common control—

(1) Shall not include profit for the transferring organization; but

(2) May include profit for the prime Contractor.

(d) The fixed hourly rates for services that meet the definition of commercial item at

2.101 that are transferred between divisions, subsidiaries, or affiliates of the Offeror under a common control may be the established catalog or market rate when it is the established practice of the transferring organization to price inter-organizational transfers at other than cost for commercial work of the Offeror or any division, subsidiary or affiliate of the Offeror under a common control.

Option to Extend the Term of the Contract
(FAR 52.217-9)(MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor at any time within the term of the contract, provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least thirty (30) days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed sixty (60) months.

52.217-8 Option to Extend Services. (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days before expiration.

(End of clause)

(End of Section I